Alert-Response for Distributed Surveillance: DODAF-based Services and Systems

Abobakr Y. Shahrah, M. Anwar Hossain and Abdullah S. Alghamdi
Software Engineering Deptartment
College of Computer and Information Sciences
King Saud University, Riyadh, KSA
Email: {shahrah, mahossain, ghamdi}@ksu.edu.sa

***Abstract*—Over decades of research and development in surveillance domain, multimedia surveillance systems have achieved a great maturity level. However, due to the distribution of surveillance capabilities in current surveillance systems, new challenges on how to manage and coordinate alerts and responses among the distributed parties becomes a challenge. These alerts and responses are the two very important information items in establishing effective collaboration among the distributed smart surveillance systems. This research aims to develop a enterprise-scale alert-response management framework based on DODAF 2.0 services and systems model. The proposed framework may be considered as generic information assimilation and coordination framework for different surveillance scenarios.**

***Keywords*—Multimedia surveillance, alert, response, enterprise architecture, DODAF 2.0**

I. Introduction

Surveillance systems [1], [2], [3] are one of the well-known multimedia-based applications which have provided a great impact on the human life in different environments and uses; starting from the simple home security monitoring system located into a single location up to a complicated system of systems (SoS) distributed over wide-area and isolated places to serve in emergency and battlefield situations. Such evolution has extended the capabilities of the surveillance systems and consequently increased its complexity.

Recently, with the significant improvements of implementing complex systems which have been spread and deployed ubiquitously and over heterogeneous platforms, 3rd generation of distributed surveillance systems [1] have evolved. In contrast to the earlier generations which had received massive research efforts and works, the new trend of the 3rd generation still under construction and has lack of considerations and formalizations. One of the major issues in such systems is the effective management of alerts and responses for distributed surveillance sites to promote collaboration among all sites for improved situation awareness and control.

Existing research in this domain focus on aspects such as common event modeling [4], frameworks and architectures [5], alert classification [6], and situation awareness [7], which will be discussed in the next section. As will be seen that these works although cover a wide range of relevant aspects, no representative research has focused on enterprise-scale alert-response management using standard enterprise architecture framework.

This work is an extension of our earlier work [8] that illustrated a collaboration architecture using several high-level DODAF models, such as High-Level Operational Concept Graphic (OV-1), Event-Trace Descriptions (OV-6c) and Logical Data Model (DIV-2). The current version specifically focuses on DODAF 2.0 [9] services and systems modeling aspects. The remainder of this paper is organized as follows: literature review appears in Section II; the proposed alert-response framework is illustrated in Section III, followed by an application scenario in Section IV. The architectural data exchange is reported in Section V, and the paper concludes in Section VI with a note to future work directions.

II. Literature Review

In this section we briefly comment on some relevant research. A common event model is proposed by authors in [4] that described the essential requirements and characteristics for developing such as a model. The aim is to facilitate and standardize the interoperability between the different types of multimedia applications. It is expected that the proposed model will provide a unified infrastructure for events processing, sorting, retrieval, and propagation.

It is essential to have standard frameworks and architectures on which surveillance systems can be built. Authors in [5] used static service-oriented architecture (SOA) and event-driven architecture to propose a framework for distributed surveillance systems. An example of using SOA to share and communicate real-time information for emergency medical response is reported in [10]. This architecture demonstrates a producer-consumer paradigm, where it integrates three systems and three new data sources to enable the interested parties in getting and distributing the required information to deal with emergencies situations.

The authors in [6] classify and describe the different types of alerts in smart surveillance systems, including real-time alerts (user-defined or automatic alerts), automatic forensic video retrieval (AFVR) that uses indexing retrieval techniques like spatio-temporal and video mining, and situation awareness for effective monitoring and high level of security.

Situation is another important aspect of distributed surveillance systems, which is studied in [7]. The study explores the diverse technologies being used in smart surveillance systems –IBM S3, PeopleVision – for object detection, tracking, classifying, storing and querying. It shows the basic architecture of such systems in addition to the evaluation and

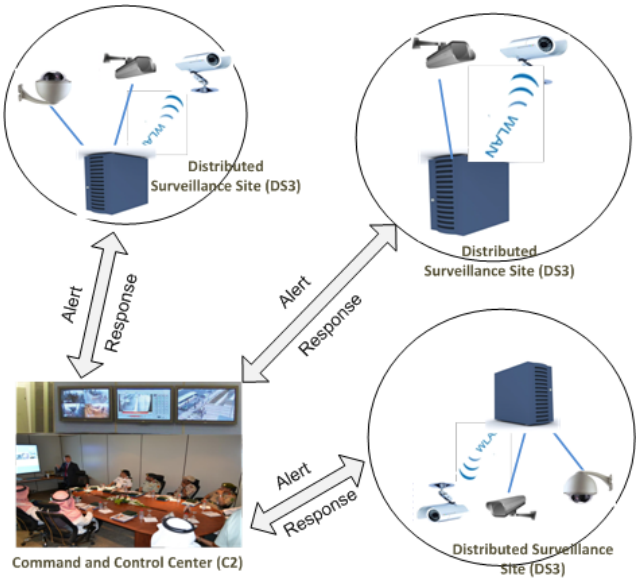

Fig. 1. Alert-Response Scenario in Distributed Surveillance Systems (OV-1)

performance measurements of situation awareness. The IBM Smart Surveillance System (S3-R1) [11] consists of two main components– Smart Surveillance Engine (SSE) which provides the front-end analysis capabilities and Middleware for Large Scale Surveillance (MILS) which provides data management capabilities. The three main features in that system includes real time notification, event retrieval, and event statistics.

Despite the presence of several research in surveillance domain, there is still no representative work that focuses on enterprise-wide alert-response management to facilitate the data exchange and integration within the distributed smart surveillance systems. This paper aims to address this aspect.

III. Proposed Alert-Response Management Framework

In this research we consider alert-response in large-scale surveillance systems consisting of multiple sites collaborating with each other by sharing event information among them. Therefore, it is important to model alert-response functionality using professional approach such as complex systems modeling methodologies and techniques. One of the well-adopted approaches is to consider Enterprise Architecture (EA) for designing and deploying such large systems that helps the stakeholders to control and manage their system infrastructure and architectural data. We resort to DoDAF 2.0 as one of the well-known EA frameworks, which defines well-structured methodology in terms of viewpoints and models to develop effective and efficient Architectural Description.

Unlike our earlier work [8], which presented a collaboration architecture using several high-level DODAF models, such as OV-1, OV-6c and DIV-2, this paper focuses on services and systems model/viewpoint of DODAF framework to illustrate enterprise-wide alert-response functionality. However, to better comprehend the proposed model, we start by providing a high-level graphical description of the operational concept using DODAF's OV-1 model [12] as shown in Figure 1.

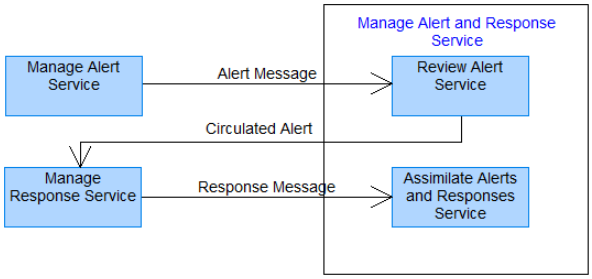

Fig. 2. Alert-Response Management in DS3 Services Context Description (SvcV-1)

Figure 1 just shows three different surveillance sites as a sample of an integrated and complicated surveillance system. In reality, such an integrated system would have more distributed sites connected. Now, before delving into the services and systems model based on the presented OV-1, we first restate the scenario of handling of alert and response in this architecture using the following steps [8]:

1) When an abnormal event is detected at any *DS3* site based on some predefined rules (e.g. fire, suspicious person or group), an alert will be generated and sent to the *C2* Center.
2) The *C2* Center receives the generated alert and makes the required analysis to verify the validity and correctness of the alert (to avoid false alerts). Then, it specifies the *Community of Interest (COI)* who are concerned and should receive this alert. Finally, circulate the alert to the relevant sites.
3) Once the intended sites receive the circulated alert sent from *C2* Center, they start the analysis and searching in their own databases for related and interested data that might have relation to the received circulated alert.
4) If any site finds interesting data related to the circulated alert, the response will be generated and sent back to the *C2* Center.
5) Ultimately, after *C2* Center receives responses from the interested sites, it starts the analysis of responses in order to have a complete awareness of the situation and end up with recommendations and action plan to control the case.

We now focus our attention to services and systems viewpoint for modeling enterprise-level alert-response management framework.

A. Services Context Description (SvcV-1)

SvcV-1 describes the identification of services, service items, and their interconnections. It addresses the composition and interaction of Services. A SvcV-1 can be used simply to depict services and sub-services and identify the Resource Flows between them [9]. Figure 2 shows the interaction of the required services in the proposed architecture and the data flows among them. It is clear from the diagram that Manage

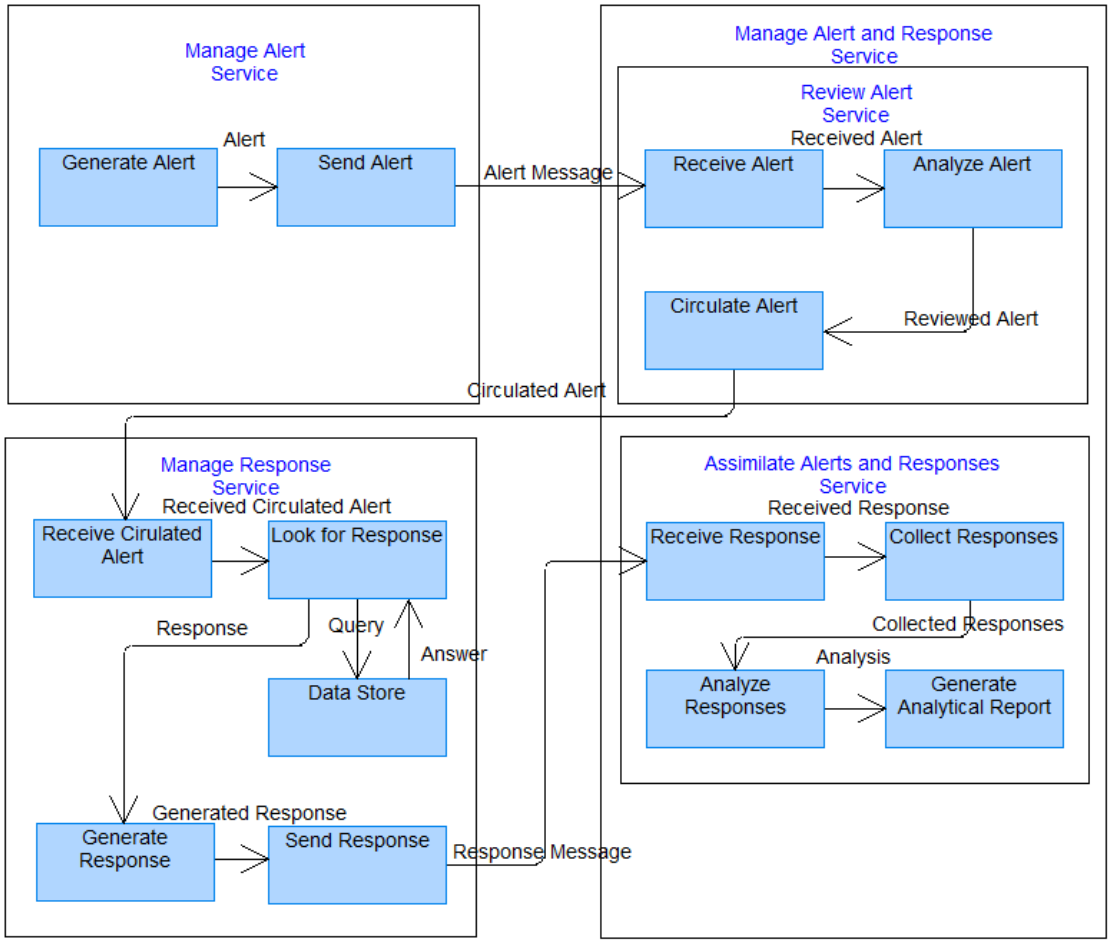

Fig. 3. Alert-Response Management in DS3 Services Functionality Description (SvcV-4)

Alert and Response service is composed of two sub-services: Review Alert and Assimilate Alerts and Responses services. The service functions for each service are illustrated in the next model (SvcV-4).

B. Services Functionality Description (SvcV-4)

SvcV-4 shows the functions performed by services and the service data flows among service functions (activities). The primary purpose of SvcV-4 is to develop a clear description of the necessary data flows that are input (consumed) by and output (produced) by each resource. This diagram depicts the data flows that flow between the services of the architecture [9]. The services required in the proposed architecture are depicted in Figure 3. This diagram is very useful for comprehending the detail of the services components and their interactions.

There are three main services: Manage Alert, Manage Response, and Manage Alert and Response. Inside Manage Alert and Response service, there are two more subservices: Review Alert and Assimilate Alerts and Responses services. The figure above shows the Service Data Flows (arrows) among Services Functions (rectangles) with specifying the messages producers and consumers within each defined services. Furthermore, the DoDAF-described Models involved in Services Viewpoints reflect the explicit support of SOA as one of evolvement in DoDAF version 2.0 for adopting the new technologies and modern trends.

C. Systems Interface Description (SV-1)

SV-1 shows the identification of systems, system items, and their interconnections. In addition to depicting Systems (Performers) and their structure, the SV-1 addresses Resource Flows. A Resource Flow, as depicted in SV-1, is an indicator that resources pass between one System and the other. The SV-1 depicts all System Resource Flows between Systems that are of interest [9]. The systems and subsystems involved in the proposed architecture are shown in Figure 4 that should be existing at each DS3 site. This diagram is a high-level of system interactions with the required data resource flows. The hierarchy structure for the systems indicates the parent (system) and children (subsystems) relationships. For instance, Alert Management and Response Management subsystems are part of DS3. C2 system has a subsystem called Alert and

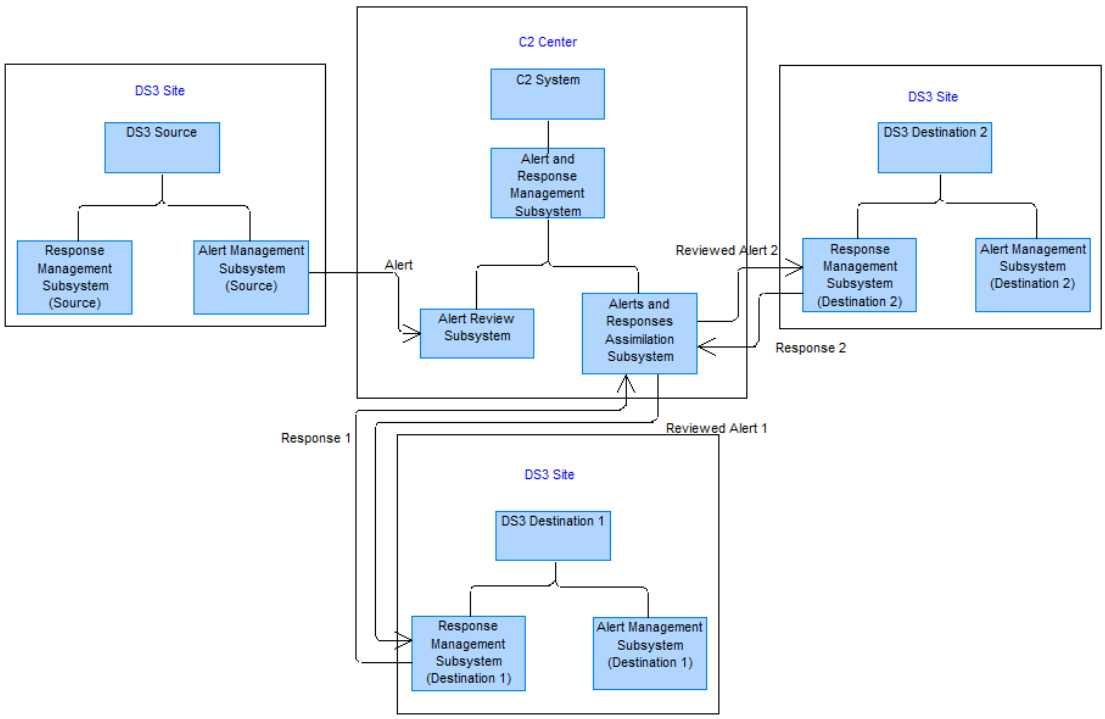

Fig. 4. Alert-Response Management in DS3 Systems Interface Description (SV-1)

Response Management subsystem which is responsible for handling alerts and responses as well as assimilating them at C2 Center.

D. Systems Functionality Description (SV-4)

The functions (activities) performed by systems and the system data flows among system functions (activities) [9]. SV-4 is very similar to that of SrvV-4 in depicting the system functionalities, but one represents systems viewpoint while the other represents services viewpoint. In terms of graphical representation, the only visible changes in SV-4 figure from SrvV-4 figure is that the high-level services of SrvV-4 are considered as subsystems in SV-4. Hence a graphical representation of SV-4 is omitted in this paper. Nevertheless, such a diagram of SV-4 can be considered as a decomposition of SV-1 into System Functions. The description of each System Functions (operational activities in OV-6c) has early been introduced in OV-6c with elaborated detail [8]. The same can be applied here by computerizing the process and exploiting the intelligent software application to accomplish the intended tasks.

In the proposed architecture, it is recommended to fully automate all the operational activities especially with the dramatic advancement in IT and computer applications supported by Artificial Intelligence (AI) and sophisticated Decision Support Systems (DSS). It can be argued that, even though, still there is a strong requirement of human involvement in the process especially for validating the alerts and responses as well as taking the final decision making, human involvement with support of present and future technologies can boost the performance and accuracy of the suggested system implementation.

Similar to the above, there are several other models for services and systems viewpoints that can be gradually developed but are omitted from here for brevity.

IV. Application Scenarios

The requirements for alert-response mechanism in distributed smart surveillance systems (DS3) become more and more pressing because of geographically spanned and complicated monitored areas, which vary from local home security to wide and distributed surveillance locations. In most cases, with traditional silos surveillance systems, it is not easy to manage such environments due to limitation in consolidated data and processing capabilities. This yields various and worthy implementation domains for the integrated smart surveillance systems applications which can be utilized in many security and civil aspects.

In order to demonstrate the proposed architecture, we present an example **wanted person scenario** step-by-step according to the described process in previous sections to simplify the understanding of the required activities associated with proposed architecture. The scenario is presented as follows:

Security agencies and other governmental bodies are usually interested in looking for and tracking particular person(s) who are suspected or associated with criminal activities. Of course, if the integration of DS3 is there, the life will be

easier and such requirements can be satisfied efficiently and effectively especially for real-time events management requirements. Otherwise, it is so difficult and time and resource consuming to physically identify and monitor individuals and sometimes group of people moving here and there. In this subsection, the wanted person scenario is described in detail as follows:

- It is assumed that, DS3 is able to identify and track a wanted person based on its intelligent components like rule-based events or image and image processing capabilities. Therefore, once a wanted person is identified, the DS3 generates an alert event with the required details to the C2 system. The generated event details can be like event ID, event name, event description, event date and time and so forth.
- When C2 receives the generated event, there should be a manual check for the event validation to avoid any false alarms distribution. Then, community of interest (COI) should be specified to receive the generated alarm. After that, C2 should circulate the generated alarm to all the specified COI.
- After the generated alert circulation done in the previous step, the DS3 receives the generated alert and starts the response processing. Usually, the response can fall into three various activities: readiness, search and monitoring. Readiness activity is a type of notification to DS3 to be in stand-by mode to expect the wanted person presence any time. This gives the DS3 the ability to prepare action plan for suspicious activities probably associated with the wanted person(s) like parallel attacks or spying activities. Search activity includes the query on the surveillance databases for possible information related to the wanted person like last time visits, activities, accompanied persons, and so forth. In fact, the DS3 response time relies on its searching and processing capabilities in terms of hardware and software infrastructure to be able to respond to the C2 regarding the received alerts in timely manner. Monitoring activity can be used to keep track of the wanted person movements especially if there are no sufficient information about the wanted person activities. In addition, this activity is the most complicated and resource consuming because of real-time processing requirements to track and show only the interested scenes related to the wanted person who crosses from one DS3 to another. The output from these three activities should be sent back to the C2 through response messages or sometimes as continuous streaming data (like in case of real-time monitoring activity).
- Ultimately, once C2 starts receiving the responses from all different COI DS3, the responses consolidation process takes place to assimilate and analyze the received responses related to the wanted person. This data will definitely assist in increasing situation awareness and preparing an appropriate action plan for dealing with such wanted person. Moreover, the responses consolidated data can be sent back as a response to the generated alert initiator if required.

```
<Name>Event-Trace Descriptions (OV-6c)</
    Name>
<Identity>487</Identity>
<prp_DGX-spa-File-spa-Name>D0000026.DGX<
    /prp_DGX-spa-File-spa-Name>
<prp_Initial-spa-Date>20110522</
    prp_Initial-spa-Date>
<prp_GUID>1cff2567-c4b2-4730-8774-3
    a0c0357043a</prp_GUID>
<prp_Initial-spa-Audit>1</prp_Initial-
    spa-Audit>
<prp_Initial-spa-Time>102607</
    prp_Initial-spa-Time>
<prp_Description>
</prp_Description>
<prp_Vertical-spa-Pools-spa-and-spa-
    Lanes>F</prp_Vertical-spa-Pools-spa-
    and-spa-Lanes>
<prp_Check-spa-Connections>F</prp_Check-
    spa-Connections>
<prp_Describes-spa-Process>
```

Fig. 5. Architecture description metadata in XML

V. Architectural Data Exchange

One of the most important aspect of developing architectural description data is the ability to exchange and manage it in a toolset-agnostic manner. So it should be a compulsory feature for good toolsets to enable the data transformation from one encyclopedia or toolset to another. This allows the analysis, optimization, and storage of architectural data based on the different requirements of the users and available toolset functionalities. In fact, this cannot be achieved without a standard format or schema definition, which ensures the common understanding and utilization of such data. For this reason, DoDAF 2.0 defines specifications for the exchange in the form of XML Schema Definition (XSD) called DM2 PES XML schema (XSD) [12], which can be shared with stakeholders of the architecture. Figure 5 shows a snapshot of the xml schema representing the DODAF based architecture description metadata.

VI. Conclusion and Future Work

This paper described an enterprise-wide alert-response management framework for distributed multimedia surveillance systems with an aim to support effective collaboration and improved situation awareness. The alert-response framework has been modeled using DODAF 2.0 architecture framework focusing on services and systems viewpoint. The proposed framework is generic enough to be applied in different application scenarios, such as battlefield and war fighting planning, combating terrorism, etc. Our future research will focus on real-life implementation and experimentation with the proposed framework. Besides, we would like to investigate on distributed command and control system for distributed surveillance systems deployed in different sites.

ACKNOWLEDGMENT

This work was supported by the Research Center of College of Computer and Information Sciences, King Saud Univer- sity, Riyadh, Saudi Arabia, through the research Project No. RC120918. The authors are grateful for this support.

REFERENCES

[1] M. Valera and S. Velastin, "Intelligent distributed surveillance systems: a review," *Vision, Image and Signal Processing, IEE Proceedings* -, vol. 152, no. 2, pp. 192 – 204, april 2005.

[2] R. Cucchiara, "Multimedia surveillance systems," in *Proceedings of the third ACM international workshop on Video surveillance & sensor networks*, ser. VSSN '05, 2005, pp. 3–10.

[3] H. M. Dee and S. A. Velastin, "How close are we to solving the problem of automated visual surveillance?: A review of real-world surveillance, scientific progress and evaluative mechanisms," *Mach. Vision Appl.*, vol. 19, pp. 329–343, September 2008.

[4] U. Westermann and R. Jain, "Toward a common event model for multimedia applications," *IEEE MultiMedia*, vol. 14, pp. 19–29, January 2007.

[5] R. Vezzani and R. Cucchiara, "Event driven software architecture for multi-camera and distributed surveillance research systems," in *Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference on*, june 2010, pp. 1 –8.

[6] A. Hampapur, L. Brown, J. Connell, S. Pankanti, A. Senior, and Y. Tian, "Smart surveillance: applications, technologies and implications," in *Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference on*, vol. 2, dec. 2003, pp. 1133 – 1138 vol.2.

[7] A. Hampapur, L. Brown, J. Connell, A. Ekin, N. Haas, M. Lu, H. Merkl, and S. Pankanti, "Smart video surveillance: exploring the concept of multiscale spatiotemporal tracking," *Signal Processing Magazine, IEEE*, vol. 22, no. 2, pp. 38 – 51, march 2005.

[8] A. Shahrah, M. Hossain, and A. Alghamdi, "A collaboration architecture for distributed smart surveillance systems based on dodaf 2.0," in *Computer Science and Software Engineering (JCSSE), 2012 International Joint Conference on*, 2012, pp. 305–310.

[9] "DoD architecture framework version 2.0 official website," DoD, 2011. [Online]. Available: http://dodcio.defense.gov/dodaf20

[10] L. Hauenstein, T. Gao, T. W. Sze, D. Crawford, A. Alm, and D. White, "A cross-functional service-oriented architecture to support real-time information exchange in emergency medical response," in *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, vol. Supplement, 30 2006-sept. 3 2006, pp. 6478 –6481.

[11] Y. Tian, "S3-r1: the ibm smart surveillance system release 1," in *Wireless and Optical Communications, 2005. 14th Annual WOCC 2005. International Conference on*, april 2005, p. 98.

[12] S. Lee and P. Johnson, "Dodaf v2.0 in action: Search and rescue (SAR) example," DoDAF Journal, 2011.