SPUTERS

(Secure Progressively Updatable Traffic Emergency Response System)

A state of the art Role Based Traffic Surveillance and XML based Emergency Response System

Product Development Plan

Author: Dr. Naren Kodali
COO – Bytefield Inc

Author	Version	Phase	Date	Comments
Naren Kodali	1.0	Phase 1	09/01/2016	Initial Writeup
Naren Kodali, Valentin Prudius	1.1	Phase 1	10/11/2016	Revisions
Naren Kodali	1.2	Phase 1	12/09/2016	Revisions

TABLE OF CONTENTS

Existing recruiting and Staffing business processes and work-flows documented reviewed and approved.	October 01, 2016	Completed
Functional requirements and use cases documented, reviewed and signed off.	February 20, 2016	Initiated/In Progress
Application software developed using the Rational Unified Process	June 2017– December 2018	Not yet Started
Multiple Iterations using the iterative and incremental model of Software Development	Jan 2017 – June 2019	Not yet Started
Code ready for Integrated, End to End Quality Assurance	July 2019	No Status
Application software QA completed, bug fixes implemented and integrated by August 2018	August 2019	No Status
System and user documentation	August 2019	No Status
System in production	September 2019	No Status

EXECUTIVE SUMMARY

Bytefield (established in Virginia in 2007) is a consulting, staffing and product development firm focused on serving mid-size government and non-governmental organizations. Bytefield has been involved in the development of IT solutions in the Education and Security domain through in-house development and strategic partnerships with external clients that use our services to develop all or parts of bigger projects. Our consultants are well versed in these domains and have strong business knowledge and the capability to comprehend and implement state of the art technology solutions in the aforementioned domains. Our service and development methodology is tailored from our educational background, academic research and prototype development that subsume the best practices and industry experience. Bytefield has consistently helped mid-level organizations define processes, controls, roles & responsibilities and artifacts aligned with their business strategy and customer needs.

In this document, we present a product development for SPUTERS (Secure Progressively Updatable Traffic Emergency Response System), a framework for traffic surveillance in crash-prone areas under normal operating conditions and incident management and emergency response during traffic accidents. This is a proprietary idea backed with multiple (10 years) of academic research, publication and prototype implementation. In its exploration Bytefield believes that similar comprehensive products do not exist to date and there is a very exclusive need for the proposed architecture in home-owner regulated localities, high rises, apartment complexes, and local governments all over the Unites States and other countries.

SPUTERS is an idea conceptualized by the COO of Bytefield (Naren Kodali) as part of his PhD Thesis and widely accepted in the academia and the pertinent industries as a viable solution in the domain of traffic surveillance and role based emergency management. The basic idea is that the proposed system (SPUTERS) uses a collection of cameras, sensors to gather video, audio and textual information. The information is used for analysis and proactive countermeasures. During emergencies, secure transmission with progressive updates along the response chain providing situational awareness to those who must orchestrate responses to incidents. SPUTERS safeguards the privacy rights of involved individuals by both

preventing privileged information from being leaked to unauthorized persons and maintaining data integrity by preventing unauthorized alteration of data flowing between incident-service providers. In order to do so, SPUTERS uses a role-based access control system that restricts a person's access to information based on the roles that person plays during an incident. SPUTERS uses a symmetric key encryption algorithm to safeguard data during transit between roles.

INTRODUCTION

The road instrumentation that is currently used for data collection purposes is inadequate and not in pace with practical solutions that can be provided with advances in intelligent transportation systems. The data-collection devices are limited to measurements such as volume, speed and occupancy. In this product specification, titled SPUTERS, we present an easily deployable, low-cost data collection and surveillance system that can be used for measuring detailed traffic data such as individual speeds, density, and other factors under normal operating conditions and act as an incident-response system in case of an emergency. This system is a collection of audio and video capturing devices, traffic sensors, and secure wireless communication networks for data transmission. We present a surveillance system with which users can retrieve live and pre-recorded surveillance video from any roadway locations under surveillance through wire/wireless web or remote display devices.

Two key high-level requirements underlying the conceptualization of the surveillance system are the following:

1. To provide low-cost innovative solutions for identifying causes of crashes in crash-prone locations and developing an accident avoidance/prevention system
2. To coordinate emergency response in the case of an incident.

The first requirement can be achieved by recording accidents and extracting traffic detector measurements that then can be used for understanding crash dynamics and their causes. Traffic measurements such as traffic intensity and quality of flow can be derived from the raw data and analyzed in order to determine crash-prone condition patterns. The second requirement necessitates a coordinated effort between many cooperating parties, including but not limited to the following: police, fire and ambulance crews, emergency room staff, wrecker services, and traffic management center (TMC) personnel.

Incident management encompasses coordinating the following types of services: emergency response, traffic control, and post-incident cleanup. Currently, a grid of handheld audio devices aids such efforts, rarely supplemented by advanced camera assemblies. Due to the fact that the visual dimension significantly contributes to situational awareness for incident management over its auditory counterpart, we propose a system of appropriately placed cameras transmitting data about unravelling events associated with incidents to traffic management and emergency response centers; we refer to this system as SPUTERS. SPUTERS is a bimodal system in that it can also be used for traffic surveillance under incident-free operating conditions.

The different views of an incident, as provided by the cameras and other sources, must be protected from unauthorized disclosure as dictated by security and privacy laws. Although security mechanisms cannot be devised to guarantee the protection of privacy, they can be used to control access by the people who use the information systems in which privacy-related information resides.[1] We propose that the role-based access control (RBAC) model be used for this purpose because most personnel at traffic management and incident response centers play distinct roles: the information that they need to access in order to perform the duties for these roles can be specified and enforced via security policy and automated RBAC mechanisms, respectively. Data gathered by SPUTERS can be used to undertake proactive measures that

[1] A violation of privacy occurs when a party who holds access to privileged data disseminates that data in an unauthorized manner to a third party. Once the third party has obtained the information, the originator of the information has little or no control over its further dissemination.

are based on information extracted from conventional sensors such as loops and new additions such as live feed captured using audio and video recording devices. It is low cost and implementable in both urban and rural settings. This product specification capitalizes on earlier projects with the introduction of new wireless-detection and surveillance-device technology.

PROPOSED ARCHITECTURE SUMMARY

The proposed framework requires appropriately placed cameras able to record both voice and video at strategic locations that are under surveillance. Frequent accident zones that show a high potential for accidents even under normal traffic flow are good candidates for deployment of SPUTERS. We envision having multiple cameras positioned at different angles simultaneously recording an unfolding incident, revealing the total scene from multiple perspectives. These real-time multimedia feeds can be combined and processed into a real-time interactive three-dimensional video for incident-time decision-making and post-accident analysis. Criteria have been proposed to reduce the likelihood of accidents occurring (Beymer et al., 1997; McLauchlan et al., 1997). Network models on intelligent urban transportation and their implications have been discussed (Ran, B. et al., 1994). Vehicle-control systems have been proposed that alert vehicles in close proximity when of minimum vehicle-to-vehicle safe-following distances are violated (Michael et al., 1998). In addition, accident probabilities, issues, and parameters related to dispatch delays in traffic incidents have been investigated (Hall, R.W., 2002). SPUTERS uses ideas and results from the previous work stated above in fine-tuning the proposed system which integrates incident-management and emergency-response intelligent transportation systems (ITS) services. SPUTERS complies with guidelines for emergency response situations that have been recommended by the US Department of Transportation (ERG, 2000). It has similar objectives to those set forth in the Automated Highway System (e.g., see Hall, Tsao, and Botha, 2002) and Anaheim (McNally et al., 1999) projects. Providing the aforementioned capabilities introduces technical challenges. Tradeoffs and compromises need to be made in order to integrate legacy and new components into an advanced traffic-monitoring system-of-systems.[2] These tradeoffs need to be evaluated in light of *quality-to-effectiveness tradeoffs* of enhanced quality-of-service (QoS) parameters (Wijesekera, D. et al., 1996) associated with scanning and stereoscopy by cameras. The proposed services in SPUTERS support numerous audio and video streams, which in turn require high-performance communication bandwidth, primary and secondary storage, and processing power to accommodate tasks such as stream acquisition. The quality of these services must ultimately match, to the extent possible, the qualitative QoS requirements as specified by the users of SPUTERS. SPUTERS supports the individual usage and sharing of multimedia documents by incident-management and emergency-response personnel. In SPUTERS, we format multimedia documents using Synchronized Multimedia Integration Language (SMIL) (Ayers, J. et al., 2001). SMIL is an XML-like markup language for integrating real-time media data.[3]This architecture is in the proposal and product specification stage, but variations with limited functionality encompassing measurement gathering have been deployed by government agencies as discussed in later sections. The major operational aspect that separates SPUTERS from other similar applications is that it captures both video and audio data in addition to providing seamless transmission while enforcing access control. Moreover, the ability to progressively and periodically update data with the use of interactive display devices while maintaining quality of service is a distinct contribution of SPUTERS to Intelligent Transportation Systems.

RELATED MARKET ANALYSIS and RESEARCH

---

[2] A system-of-systems is a federation of legacy systems and developing systems that provide an enhanced capability greater than that of any of the individual systems within the system-of-systems.

[3] Extensible Markup Language (XML) is used to structure Web documents, that is, for defining document types.

Most of the current surveillance systems do not provide improved access to data to support decision making by using an integrated and progressively updatable knowledge base. They are mostly legacy systems with fixed workflow and process orientation and do not allow for the upgradation of technology and infrastructure. We have studied reports that conduct an independent analysis of implementation costs, durations and the achievement of implementation benefits from both domestic HOA associations, high rise residential architectures and apartment complexes of varying sizes. Bytefield has also surveyed and tested multiple COTS (Commercial off the Shelf) products and concluded that comprehensive implementation is mostly limited to gathering information for after the face post incident/accident scenarios while ignoring several unique benefits achieved through the real-time accumulation and dissemination of live audio, video and text data that emanates from the capturing devices that are constantly collecting and storing information. Additionally, the ongoing cost of maintaining existing customizations, and ensuring they operate after upgrades, will continue to cost significant amounts of money and therefore it is imperative that such needs are replaced with comprehensive enterprise wide solutions with integrated architectures that can be implemented with universal languages such as XML and its variants in this case (SMIL) over open source platforms.

It is the belief of Bytefield the SPUTERS will enable the establishment of these core values and assists the strategic goals of content based surveillance and emergency response and the delivery of its programs. The success of the proposed integrated solution is largely due to the prudent and phased implementation approach, in contrast to the “big-bang” approach. The integrated and progressively updatable emergency response system functionality can be gradually enhanced and expanded through the implementation of additional portfolio of projects to include missing required functional blocks based on the surveillance and post incident workflow. SPUTERS has a distributed multi-participant client-server architecture designed to permit multiple users to share media streams within a networked environment; this architecture was originally proposed by (Schmidt, B.K., 1999). Multimedia streams, consisting of audio and video originating from various sources are combined to provide media clips that accommodate look-around capabilities. The architecture is interactive; that is, clients can interact with the server to negotiate levels of QoS. In an ongoing project conducted by the University of Minnesota (Minnesota, ITS Institute) related to crash prevention and the detection of crash-prone conditions, a location in Minnesota was heavily instrumented, observed, and analyzed. Between September 2014 and 2015, more than 150 crashes occurred on this stretch of highway (95 of them captured on video), ranging from rear-end collisions to multi-vehicle crashes with injuries. In addition, 215 near misses have also been recorded at the same location. These data show that crashes occur under certain traffic conditions that can be detected prior to a crash occurring. The goal of this research is to provide low-cost innovative solutions for identifying causes of crashes in crash-prone freeway locations and developing an accident avoidance/prevention system.

The growing trend toward wireless transmission of traffic data places stringent constraints on the transmission of image and video data over low-speed wireless channels, such as CDPT (Cellular Data Packet Transmission). This research has explored several interconnected technical and system integration issues related to practical implementation of wireless audio/video transmission. There are commercial products that provide for transmission of audio/video data. However, SPUTERS relies on real-time delivery of audio/video data. To achieve adequate storage and retrieval of recorded data and for transmission over low-bandwidth Internet connections and wireless connections, tradeoffs must be made between the amount of data to be transmitted and the overall quality of service (e.g., security of data during transmission). For instance, security mechanisms introduce nontrivial amounts of communication, computational, and storage overhead with the potential to reduce the quality of service afforded by an ITS. SPUTERS provides practical transmission of multiple video streams over limited-bandwidth communication channels; this includes transmission over limited-bandwidth wireless channels, as well as transmission over fixed-link channels where the bandwidth requirements exceed available link capacity.

Mitretek implemented an XML/XSL, form-based emergency-response application. Updates that are a part of the emergency response are handled by a central authority; the authority controls the transmissions to various clients located at the distributed call centers. In contrast to SPUTERS, the Mitretek system does not employ real-time video, relying instead on transferring data through text-based messages. A statewide camera installation on freeways to capture live images for traffic surveillance has been undertaken by the Washington State Department of Transformation (WSDOT); the public can access these images via WSDOT's Website. However, WSDOT's cameras produce images as opposed to real-time media. In contrast, the California PATH Program has successfully field tested the Anaheim Advanced Traffic Control System and afforded the transmission of real-time data about traffic patterns and incident management.

Certain existing techniques address techniques to track individual vehicles across multiple detector stations to obtain real-time path-flow data such as travel time and volume. Their findings serve as a logical and necessary precursor to possible field implementation of vehicle reidentification techniques. The methodology, designed to evaluate a traffic surveillance system using microscopic traffic simulation, can be used to analyze the performance of SPUTERS. Wireless geo-location information added with real-time audio/video has the potential to advance traffic management efforts significantly and at a relatively low cost when compared with conventional intelligent infrastructure. The Federal Communications Commission's (FCC) E911 regulations require that wireless phones incorporate geo-location technology (i.e., GPS) to facilitate the accurate location of the origin of wireless 911 calls. Vehicles with active wireless phones can extend the existing surveillance range; the percentage of new vehicles with wireless communications is forecast to grow dramatically over the next ten years. Functional systems of this nature are deployed in Baltimore and Washington, D.C. metropolitan areas. The Maryland State Highway Administration and FHWA have a contract with U.S. Wireless to provide wireless surveillance. In Hampton Roads and Virginia Beach, Virginia, U.S private entities have partnered to develop a wireless geo-location ATIS system for the Virginia Department of Transportation (VDOT).

SPUTERS is based on SMIL, a W3C standard for multimedia as an extension of XML. SMIL formatted documents are considered as semi-structured data. Now, we briefly survey the state of the art regarding secure processing of semi-structured documents. Controlling access to XML documents of a textual nature attracted widespread interest since XML became one of the *de facto* standards for use on the World Wide Web (WWW). Evolving multimedia has a sense of continuity and inter-media synchronization embedded in it. The audio, video as well as text and images, play out in a predetermined order bound by time. (Kodali et al., 2002; Kodali et al., 2003) have proposed architectures for multimedia applications such as secure pay-per-view movies and electronic surveillance of facilities with multi-level security (MLS) requirements. The usage of the granular structure of SMIL to provide real-time secure traffic surveillance for both incident management and emergency response was initially suggested by (Kodali et al., 2002). In SPUTERS, the traffic model is enhanced for progressive updates and interactivity between participating clients.

AN INTEGRATED TRAFFIC SURVEILLANCE AND EMERGENCY RESPONSE ARCHITECTURE

SPUTERS (Secure Progressively Updatable Traffic Emergency Response System) is a framework for traffic surveillance in crash-prone areas under normal operating conditions and incident management and emergency response during traffic accidents. SPUTERS uses a collection of cameras, sensors to gather video, audio and textual information. The information is used for analysis and proactive countermeasures. During emergencies, secure transmission with progressive updates along the response chain providing situational awareness to those who must orchestrate responses to incidents. SPUTERS safeguards the privacy rights of involved individuals by both preventing privileged information from being leaked to unauthorized persons and maintaining data integrity by preventing unauthorized alteration of data flowing between incident-service providers. In order to do so, SPUTERS uses a role-based access control system that restricts a person's access to information based on the roles that person plays during an incident. SPUTERS uses a symmetric key encryption algorithm to safeguard data during transit between roles.

A RUNNING EXAMPLE

To explain the intended functionality of SPUTERS, we introduce a case study in which multiple cameras and microphones are used to capture incidents on roadways within a city where the frequency of incidents is high. The city would have to install multiple cameras (i.e., surveillance stations) that continuously provide real-time audio and video for physical surveillance in addition to data collected via conventional surveillance systems (e.g., traffic speed measured via inductive loops embedded in the pavement). An Emergency Help Center (EHC) is created wherein the feeds from the camera and audio devices are received and processed. Suppose that every vehicle registered to a location within the city limits is a mandatory subscriber and the following two conditions are satisfied:

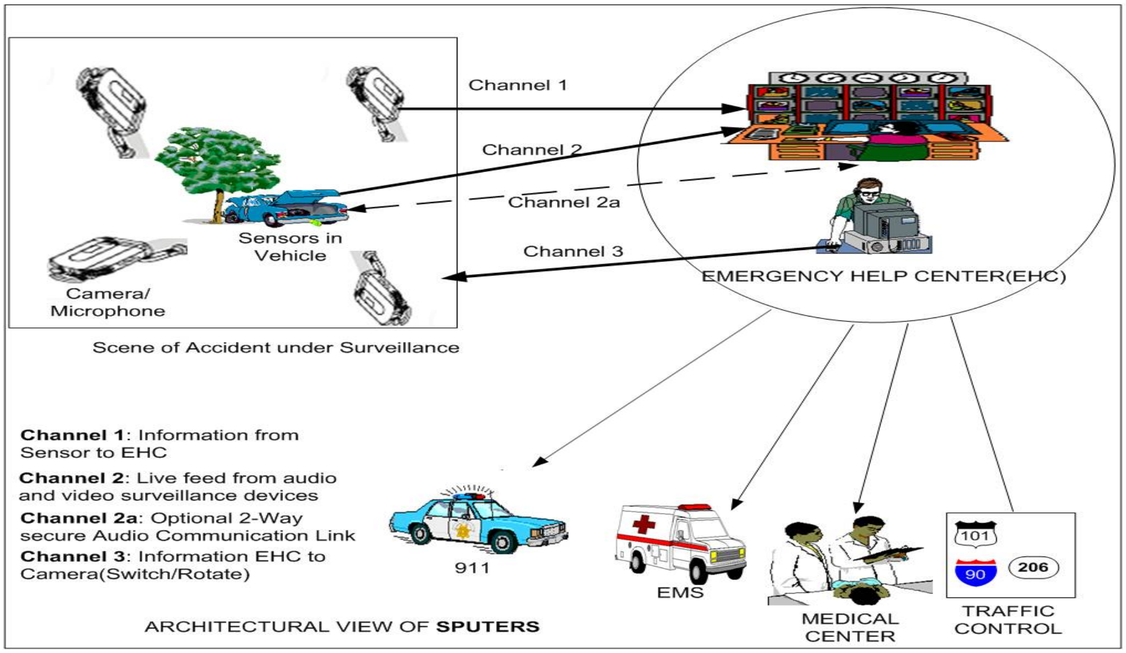

Figure 1: Architectural view of SPUTERS.

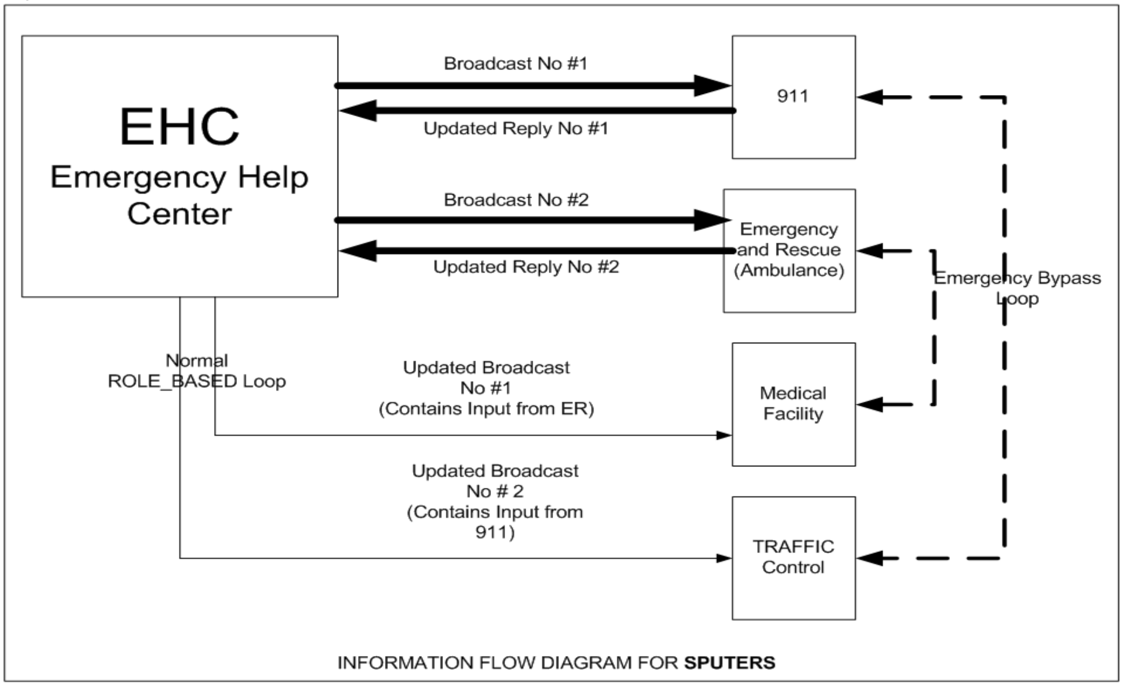

Figure 2: Information Flow Diagram for SPUTERS.

1. Each individual subscriber vehicle has *sensors* detecting and recording vehicle status before, during, and after the incident using parameters such as change in velocity, angle of impact, airbag deployment, rollover, and at-rest (i.e., ending) position. These sensors and/or wireless cellular devices reveal the geographical location of the incident via GPS coordinates of the subscriber vehicle.

2. At service initiation, users are required to provide some personal and medical information such as age, domicile, blood type, and point of contact in case of an emergency; this information is stored in a database. EHC personnel depending on the roles they play, such as 911-dispatcher, police officer, paramedic, and traffic-management controller can access specific types of data in the database. The EHC accesses some of this data and maps it to classes of potential users in accordance with rights, requests and privileges of subscribers, resulting in the establishment of an *access control list* (ACL).

When there is no incident, the surveillance station gathers the following information:

- Traffic speed, density and volume
- Driving patterns
- Rush hour dynamics
- Frequency of potential, but avoided incidents

When an incident occurs, the surveillance station gathers the following additional information as shown in Figure 1:

- Data from vehicle sensors
- Live video feeds from multiple cameras as the situation unfolds
- Real-time audio associated with cellular devices or secure audio lines
- The GPS coordinates of the location of the incident

SPUTERS relies on conventional sensors to gather measurements such as traffic speed, volume and intensity to supplement situational awareness data gathered via organic sensor and communications mechanisms. The preliminary task of the EHC is to add vehicle information and medical data about the probable or confirmed occupants of the vehicle from its database. The secondary task is to gather and provide real-time traffic information about current congestion and road conditions, and report them to pre-determined recipients. All real-time media feeds and other forms of valuable information obtained are sent to the EHC through secure and dedicated channels as soon as an incident occurs. Sensor information and alarms can be used to dispatch emergency-response personnel in a timely manner. Feeds from cameras and microphones are used to aid in time-critical emergency decision-making and post-incident forensic analysis. The medical data must have been provided in advance by the EHC subscriber, with the provision that it will be released to appropriate medical personnel only in emergencies.

All media components that arrive at the EHC are integrated and synchronized into SMIL media files. The same SMIL file is passed from each location to the next in sequence, while safeguarding the subscriber privileges by controlling access to private information. All transmissions of data files between intermediate stations in the network use standard hypertext transfer protocol (HTTP). Personnel can open a standard Web browser window to receive data files. The EHC can send information to multiple clients simultaneously. Our example has four clients, which perform mutually diverse activities within the scope of emergency responses, classified by the *role* they play; the client and their composite sub-entities are as follows:

1) **911** (Control Room/Law enforcement officers, patrol officers)
2) **Emergency Medical Service** and Rescue Teams [EMS] (Fire, Ambulance)
3) **Medical Control** (Personal doctor/Hospital/ Emergency specialists)
4) **Traffic Control** (Traffic controllers)

In the remainder of this product specification document, the name of the client (represented in bold) is used to represent any or all of its sub-entities.

Figure 2 shows the flow of information into and from the EHC and between cooperating entities. The data flow is dependent on the role of the recipient and will be subsequently discussed along with progressive update services provided by SPUTERS.

SMIL (Synchronized Multimedia Integration Language)

SMIL is an extension to XML developed by W3C to author presentations, allowing multimedia components such as audio, video, text and images to be integrated and synchronized to form a presentation. The distinguishing features of SMIL over XML are the syntactic constructs for timing and synchronization streams with qualitative requirements. In addition, SMIL provides a syntax for spatial layout including constructs for non-textual and non-image media and hyperlink support. Here, we explain those SMIL constructs that are relevant for our application, and show how they can be used to specify a multimedia document satisfying the application needs stated in earlier sections. SMIL has <seq>, <excl> and <par> constructs for synchronizing media. They are used to specify in a hierarchical manner synchronized multimedia compositions. The <seq> element plays the child elements one after another in the specified sequential order. <excl> specifies that its children are played one child at a time, but does not impose any order. The <par> element plays all children elements as a group, allowing *parallel* play out. For example, *<par><video src=camera1><audio src = microphone1></par>* specifies that media sources camera1 and microphone1 are played in parallel.

```
<smil>
     <head>
    <layout type="text/smil-basic">
     <channel id="video1" left="20" top="50" z-index="1"/>
     <channel id="text1" left="20" top="120" z-index="1"/>
     <channel id="video2" left="150" top="50" z-index="1"/>
     <channel id="text2" left="40" top="70" z-index="1"/>
     <channel id="video3" left="60" top="120" z-index="1"/>
     <channel id="text3" left="70" top="110" z-index="1"/>
     </layout>
     </head>
   <body>
<seq>
<sensor>
<text src = "Input from SENSOR 1" channel = "text1"/>
<text src="Input from SENSOR 2 " channel="text2"/>
 </sensor>

//Input from the SENSORS implanted on the Clients automobile

<par>
<audio src = "Secure AU link " dur = "42s" channel="video2"
</par>

//In put from the Secure Direct Audio link created between
EHC and VICTIMS automobile

<seq>
     <img   src="Accident"/>
           <par>
        <camera1>
            <video src="Camera1" channel="video1"dur="45s"/>
            <audio src="Camera1 audio"/>
        </camera1>
         </par>
         <par>
        <camera2>
              <video src="Camera2 " channel="video2"/></a>
              <audio src="Camera2 audio"/>
        </camera2>
         </par>
         <par>
              <camera3>
              <video src="Camera3 video" channel="video3"/>
              <audio src="Camera3 audio"/>
              </camera3>
         </par>

 //Similarly, this is a comprehensive document with inputs
from all cameras (both audio and video)

</seq>
   </body>
</smil>
```

Figure 3: SMIL Database (All information received at EHC)

In SMIL, the time period that a media clip is played out is referred to as its *active duration*. For parallel play to be meaningful, both components must have equal active durations. For clips that do not have equal active durations, SMIL has constructs for making them equal. Some examples are *begin* (allows to begin components after a given amount of time), *dur* (controls the duration), *end* (specifies the ending time of the component with respect to the whole construct), and *repeatCount* (allows a media clip to be repeated a maximum number of times). In addition, attributes such as *syncTolerance* and *syncMaster* control runtime synchronization, and specify the tolerable mis-synchronization (e.g., as tolerable lipsynchronization delays) and a master-slave relationship between synchronized streams, respectively. In this paper, we consider only the basic forms of a synchronization construct, that is, we do not specify syncMaster and syncTolerance. We assume that components of <par> have equal play-out times and they begin and end at the same time. An important construct that we use is *<switch>*, allowing one to toggle among alternative compositions listed among its components. These alternatives are chosen based on the values taken by some application-specific attributes. For example, *<switch> <audio src="stereo.wav" systemBitrate>25><audio src="mono.wav" systemBitrate < 25></switch>* plays stereo.wav when the SMIL-defined attribute *systemBitrate* is at least 25 and *mono.wav* otherwise. We use this construct to specify our surveillance application and to enforce quality and resource negotiation between the mobile clients and the EHC.

The SMIL document given in Figure 3 provides an example of how the information received at the EHC can be combined to make a multimedia presentation. As in this example, the input from the sensors, voice link, and all available cameras are bound by structure and synchronized by time containers. In addition, there are four forms of media video, audio, text and image that are integrated and synchronized using <seq> and <par> constructs. The primitive media entity is a frame, and frames are sequenced together to form scenes. The audio, video and text frames (if any) run in parallel to combine and render a scene. Groups of scenes constitute a shot. EHC defines how many and which scenes constitute a shot. This *cinematic* structure of media is necessary for imposing rules and access constraints. In SPUTERS, the *shot* is the granularity on which we impose access control and encryption.

MULTIPARTICIPANT STEREO VIDEO

The EHC controls cameras installed at the location and is able to switch from one to another in real-time. The operator is able to rotate stationary cameras through various degrees of freedom and observe a sense of *look-around*.

```
<smil>
<body>
  <seq>
        <img   src="Media Clip: Accident No: 6345"/>
          <par>
        <shot1>
              <video src="Camera1" dur="45s"/>
              <video src="Camera3" dur="23s"/>
              <video src="Camera2" dur="4s"/>
              <audio src="Camera1 "/>
              <text src = " sensor" />
              </shot1>
         </par>
         <par>
        <shot2>
              <video src="Camera3" channel="video2"/></a>
              <audio src="Camera3 audio"/>
              <text src="sensor" dur "8s " channel="text2"/>
              </shot2>
        </par>
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (Similarly various shots with pertinent combinations as
decided by EHC are made to form the 3-d media clip)

</body>
</smil>
```

Figure 4: A Media Clip generated as a combination of "shots".

Such cameras (e.g., TRICLOPS) are commercially available. These two unique features, namely switching and rotatability, can be supervised remotely and provide a three-dimensional view with an added sense of immersion. Stereoscopic cameras provide depth perception. In effect, SPUTERS permits multiple feeds from variable reference points to be sent to the EHC. Judicious mixing of these various independent audio and video feeds, and sometimes cross-matching and combining the audio and video components of multiple mutually different but simultaneous captures, enables creating media clips that are informative for decision-making.

Figure 4 above shows a SMIL structure of a media clip generated based on the data received from the SMIL database (Figure 1) divided into shots pertinent to the role of the recipient. In <shot1>, the audio, video and text components are chosen from both different cameras and locations, yet combined together to make a sensible media clip. The same event is simultaneously captured by multiple cameras: the video in one camera could be mixed with the audio of another camera to yield interesting and valuable data—from a situational-awareness perspective—otherwise unnoticed. SMIL's integration capabilities enable emergency-response personnel to mix and match relevant parts from different media streams.

Multi-participant video would be helpful for post-incident analysis and planning for handling future incidents. In case of criminal activity, these media clips could be used as evidence in a court of law. During normal surveillance, a three-dimensional stereoscopic media file could potentially yield more decisive information, when compared with existing methodologies.

PROPOSED ROLE HIERARCHY AND PROGRESSIVE UPDATES:

As stated, EHC communicates and shares data with multiple entities depending on the role they play in emergencies; in such a case, the order of information flow is known. Figure 5 shows activities assigned to roles, and the permissions and prohibitions that are granted via ACL's to enforce separation-of-duty constraints. For example, the EMS does not receive sensor input, while the medical facility does not receive traffic details. Information such as *time since incident* is made accessible by every role, but updatable by none. Some initially unavailable parameters are marked N/A. Some information is withheld to protect an individual's privacy or because of its irrelevance to a particular role.[4] The starting point and the reconnaissance point thereafter is the EHC, but all intermediate recipients can add extra information to the document through an XML form provided with the transmitted document. Information flows during *normal conditions* and *emergency conditions* with appropriate permissions (read and write) are shown in Figure 5. Under normal conditions, the flow of information originates from the EHC, which sends data to 911 and the EMS. Both recipients send back updated information as shown in Figure 2. The EHC now sends information to the medical facility and traffic control. All the recipients (i.e., 911, EMS, Medical Control and Traffic Control) have read/write permissions and are allowed to send back updated information to the EHC. During emergencies, additional information paths are opened. Personnel at the 911 facilities are allowed to send information directly to Traffic Control for command and control of emergency vehicles. EMS is allowed to send information to the medical facility if the victims require advanced treatment or on-the-scene administration of medication. All the possible sender-receiver pairs with the appropriate permissions are tabulated in Figure 5.

Normal Conditions	Sender	Permissions	Emergency Conditions	Sender	Permissions
	READ	WRITE		READ	WRITE
EHC - 911	Yes	Yes	EHC - 911	Yes	Yes
911 - EHC	Yes	Yes	911 - EHC	Yes	Yes
EHC- EMS	Yes	Yes	911 - Traffic Control	Yes	Yes
EMS -EHC	Yes	Yes	Traffic Control -911	Yes	Yes
EHC - Medical Facility	Yes	Yes	EHC - EMS	Yes	Yes
Medical Facility -EHC	Yes	Yes	EMS - EHC	Yes	Yes
EHC - Traffic Control			EMS - Medical Facility	Yes	Yes
Traffic Control - EHC			Medical Facility - EMS	Yes	Yes
			EHC -Medical Facility	Yes	Yes
			Medical Facility - EHC	Yes	Yes
			EHC - Traffic Control	Yes	Yes
			Traffic Control - EHC	Yes	Yes

[4] The latter can be viewed as a mandatory form of information filtering in which the user has no discretion over setting his or her profile for receiving information.

		Sensor Input	Vehicle No	Victim Name	Medical Info	GPS	Traffic Details	Casualities	Congestion Info	Medical History	Time since Incident
911/Law		Yes	Yes	Yes	No	Yes	Yes	N/A	N/A	No	Yes
EMS(Ambulance)		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Medical Facility		No	No	Yes	Yes	No	No	Yes	No	Yes	Yes
Traffic Control		No	No	No	No	Yes	Yes	No	Yes	No	Yes

Figure 5: Information Flow, Roles and Permissions of the Clients in Normal/Emergency Conditions in SPUTERS.

The EHC is responsible for the smooth transition of information for providing the personnel involved in handling an incident with situational awareness. All the recipients continuously update and resend information that they receive back to the EHC.

XML FORMS AND XSL STYLESHEETS:

Forms using XML and style sheets using XSL comprise the crux of the secure information flow. In SPUTERS, a valid transmission is a role-based combination of the following:

- An integrated media clip
- A XSL style sheet corresponding to the role for the retrieval of only the appropriate shots
- A form containing information and interactive user-input slots that are dependent on the role of the recipient

Every recipient is assigned a style sheet glued to a SMIL data file. Although the same SMIL data file is transmitted, different style sheets are used to extract privileged and protected information by following an access control model. Some of the fields within the form are not visible wherever there is a need for protection or, that particular field is irrelevant to the role of the recipient. For example, medical information is shielded from the Traffic Controller, while it is made available to paramedics and firefighters. The combination of all three components listed above is broadcast in unison to the intended recipients. Figures 5a through 5d represent the forms, and the fields that are visible due to the stylesheet along with the integrated media clip for the normal operating mode. The information is displayed on the handheld or other computing device's browser window after receiving the SMIL document. Selected portions of the data are displayed in accordance with the accompanying stylesheet. Each form has the following components:

- The video visual that is rendered by the SMIL player on the display device by interpreting the integrated media clip in the transmission
- A geographical map of the incident location
- Client updatable information boxes, and additional place for notes

```
<smil>
<body>
  <seq>
     <img src="SPUTERS Media Clip for EHC-911:Acc No: 6345"/>
<par>
<text src = " sensor" />
<text src="sensor" dur "8s " channel="text2"/>
</par>
        <par>
        <shot1>
              <video src="Camera1" dur="45s"/>
              <video src="Camera6" dur="14s"/>
              <audio src="Camera3 "/>
              </shot1>
         </par>
         <par>
        <shot2>
              <video src="Camera2" channel="video3"/></a>
              <audio src="Camera6 audio"/>
              </shot2>
        </par>
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(Similarly, various shots with pertinent combinations as
decided by EHC that are valid for  911 form the 3-d media
clip)
</body>
</smil>
```

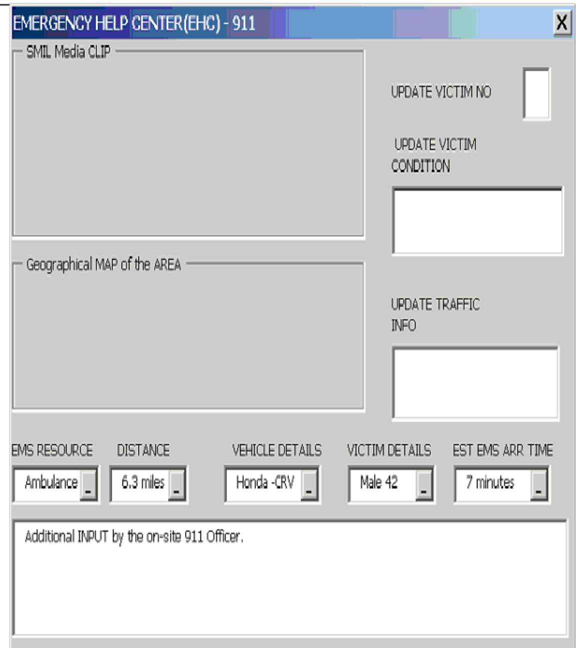

Figure 5a: SPUTERS: Media Clip for Emergency Help Center – 911

In the transmission from the EHC-911 (see Figure 5a), the police receive the transmission in the SMIL format in their handheld device, and the XSL stylesheet selects relevant portions of the data to display. Detailed information about the location of the car and its make, model, and license and the arrival information of EMS are available while no information is accessible about the medical records/history of the vehicle occupants. The number-of-victims field and victim condition could be changed by authorized on-site 911 personnel responding to the call to reflect the current condition at the site. The updated form is sent to back to the EHC or Traffic Control.

```
<smil>
<body>
  <seq>
      <img src="SPUTERS Media Clip for EHC-EMS: Acc NO:
6345"/>
          <par>
        <shot1>
              <video src="Camera1" dur="45s"/>
              <video src="Camera3" dur="23s"/>
              <video src="Camera2" dur="4s"/>
              <audio src="Camera1 "/>
              </shot1>
         </par>
         <par>
        <shot2>
              <video src="Camera3" channel="video2"/></a>
              <audio src="Camera3 audio"/>
              <text src="sensor" dur "8s " channel="text2"/>
              </shot2>
        </par>
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(Similarly, various shots with pertinent combinations as
decided by EHC that are valid for EMS form the 3-d media
clip)

</body>
</smil>
```

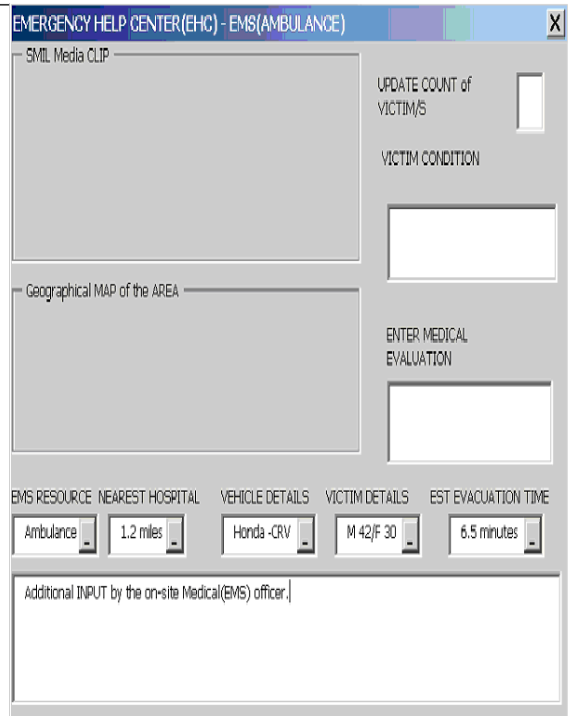

Figure 5b: SPUTERS: Media Clip for Emergency Help Center – EMS (Ambulance/Fire)

```
<smil>
<body>
  <seq>
 <img src=" SPUTERS Media Clip for EHC-Med Control:Acc No:
6345"/>
          <par>
        <shot1>
              <video src="Camera1" dur="45s"/>
              <video src="Camera3" dur="23s"/>
              <video src="Camera2" dur="4s"/>
              <audio src="Camera1 "/>
              <text src = " sensor" />
              </shot1>
        </par>
        <par>
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(Similarly, various shots with pertinent combinations as
decided by EHC that are valid for  Medical Control form the
3-d media clip)

</body>
</smil>
```

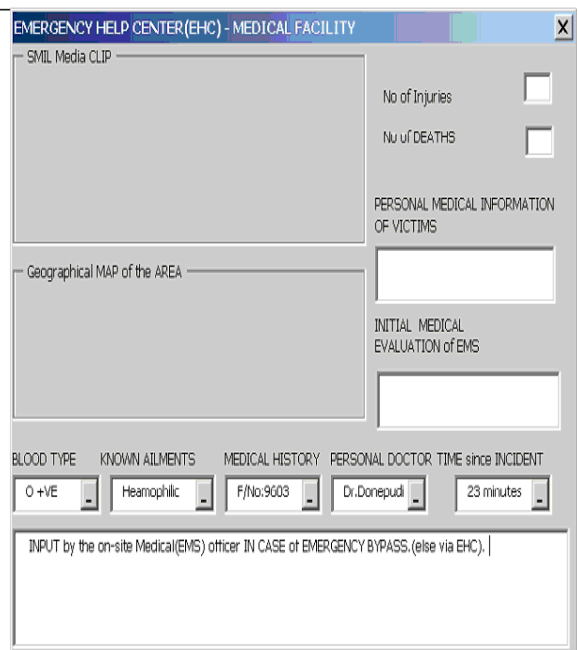

Figure 5c: SPUTERS: Media Clip for Emergency Help Center – Medical Facility

The EMS (see Figure 5b) views relevant portions of the integrated data using a stationary or a handheld SMIL-compatible device. This permits response vehicles to be immediately dispatched to the scene of an incident and sent updates about the incident while enroute. There is an uninterrupted exchange of developing information, with the emergency team primarily sending back information to the EHC in case of change/addition or new findings after reaching the scene that could not be captured otherwise. A field for medical updates and information such as nearest hospital is also provided.

After receiving the updates form 911 and EMS, the EHC transmits the media file to Medical Control (see Figure 5c). Under normal operating conditions, the dialogue is only between EHC and the EMS. However, if the condition of a victim is critical, the EMS is allowed to bypass the EHC and correspond directly with the medical facility. Such communication may involve the exchange of protected medical information such as occupant blood types, allergies, current medications, and current health, with unusual items shown to be blinking or marked urgent. Medical and contact information for each vehicle occupant is maintained in the EHC database but may not be included in data transmissions unless required and permitted by law to be seen.

```
<smil>
<body>
  <seq>
    <img src="SPUTERS Media Clip for EHC-Traffic Control: Acc
No: 6345"/>
          <par>
        <shot1>
              <video src="Camera1" dur="33s"/>
              <video src="Camera4" dur="12s"/>
              </shot1>
         </par>
         <par>
        <shot2>
              <video src="Camera2" channel="video2"/></a>
              <audio src="Camera4 audio"/>
              </shot2>
        </par>
         <par>
        <shot3>
            video src="Camera2" dur="39s"/>
            <audio src="Camera1 "/>
         </par>
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(Similarly, various shots with pertinent combinations as
decided by EHC that are valid for Traffic Control form the 3-
d media clip)
</body>
</smil>
```

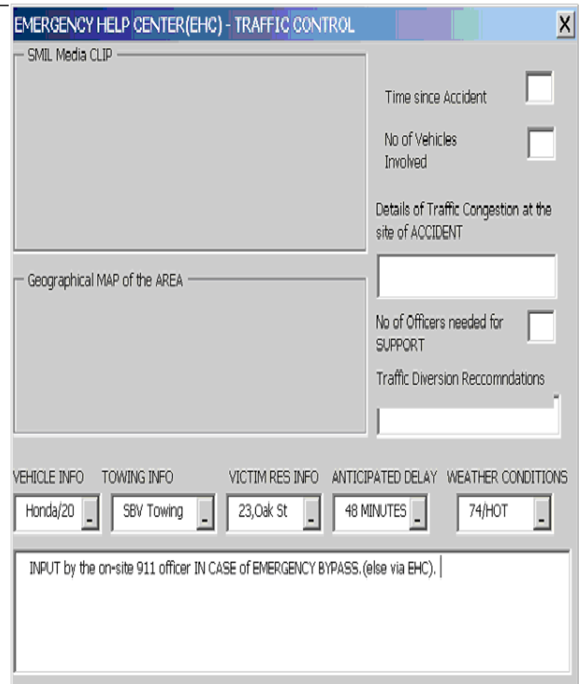

Figure 5d: SPUTERS: Media Clip for Emergency Help Center – Traffic Control

Finally, at Traffic Control, the EHC relays a periodic message with updates on the situation, with information such as stalled traffic due to the incident; time elapsed since the incident, and the estimated time to handle the incident or collision (if any). In some cases, 911 can directly communicate with traffic control and exchange information, that is, bypass the EHC.

QUALITY AND RESOURCE NEGOTIATION:

The Service Level Agreement (SLA) determines the specifications and restrictions that have to be communicated between the client and the server in order to maintain an acceptable (to the user) level of quality. The requirements of the processors, memory (primary and secondary), and other QoS parameters such as tolerable delay, loss, and image size, have to be negotiated prior or sometimes during the transfer process. HQML (Xiaohui, G. et al., 2001) proposes an XML-based language for the exchange of processor characteristics. The most important characteristic is the size of the buffer, in terms of memory that the recipient device should have, in order to maintain continuity. These specifications are represented within the SMIL document, so that the recipient device will first prepare or disqualify itself from reception. In Figure 7, resource negotiation is specified in the form of HQML tags for the handheld devices for three different recipients. Memory, delay and clarity are represented using XML syntax. On receiving this file, the mobile or stationary device makes decisions based on the user or server-defined thresholds. Figure 7 shows QoS parameters within the body of the SMIL document. These parameters are to be negotiated prior to the display. They could be set as custom SMIL-defined attributes that have to resolve to *true* during the display.

THE ACCESS CONTROL MODEL:

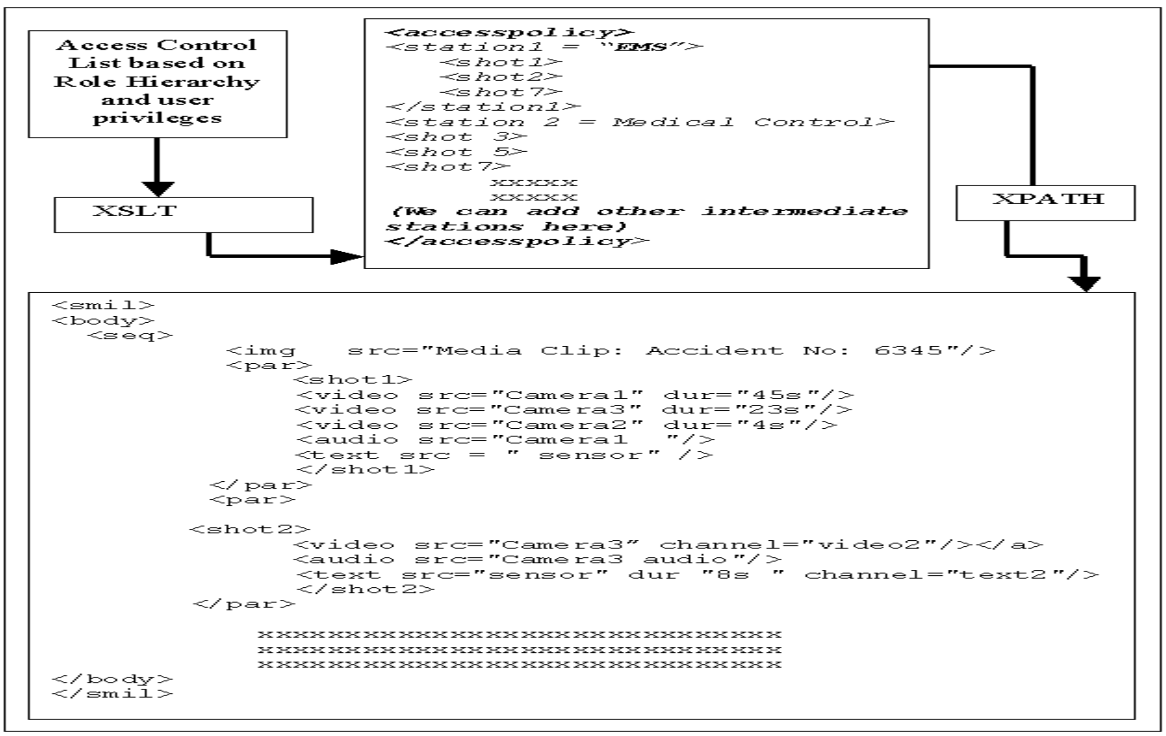

Figure 6: The Access Control Mechanics in SPUTERS.

After creating the SMIL document we need to specify authorizations in terms of *access control lists*. They are generated based on the subscriber information and their rights and preferences and the roles of the recipients. The authorization rules are formulated and represented on a XML stylesheet called XPAS (XML Policy Authorization Sheet). The time-container tags encompass the frames and scenes and the level of granularity is the shot, implying that the entire SMIL document is divided into a sequence of individual shots. Every SMIL document can be represented as a tree with *n* number of nodes. XPATH (Clark and DeRose, 1999; Clark, J., 1999) is a regular language[5] for identifying nodes of an XML document. Because the syntactic structure of SMIL is similar to XML syntax, we use XPATH to specify individual nodes. The

[5] A regular language is one that is accepted by a finite automaton.

authorization rules specify access privileges granted to the user on subscription to the service. In these rules, *subjects* are recipients of information from the EHC and are uniquely identified by the *role* they play in emergency response. An *object* is any node in a XPATH tree. Patterns are matched using regular expressions to identify objects that satisfy specified conditions.

A pattern search is run using XPATH tree to yield shots permitted to be seen by a role. An XSL Transform is used to convey the authorization rules to the SMIL document and extract the nodes that obey the authorization rules. Each role has a different stylesheet pertinent to the authorization and access privileges that it enjoys. The XSL transformation is the interface that relates the authorization stylesheet to the SMIL specification of the media clip. XSLT interprets the rules as patterns, and using XPATH, parses through the SMIL document and retrieves the appropriate shots.

THE ENCRYPTION MODEL:

The encryption model conforms to current practices used in secure broadcasting, such as bank transactions data and stock quotes over the Internet. A *smartcard*, containing the authorization rules, is installed on all recipient devices. It has a built-in parser to decrypt data as described below. The encryption model uses both symmetric and public key encryption algorithms.

Step1:
As stated, a SMIL media clip is divided into *shots*. We encrypt each shot with a unique symmetric key. All encrypted shots can be decrypted using the same key. Based on the subscriber authorization rules, a finite number of symmetric decryption keys corresponding to shots permitted to be seen by a role are grouped together as a vector of keys, termed a *keyvector*. This distinct keyvector for a particular role is required for use in decrypting all shots permitted for that role.

Step 2:
The keyvectors generated for recipients, based on their roles, are encrypted with the public key of the recipient. The encrypted keyvectors are transmitted by unicast to the recipient prior to the actual broadcast of the media clip. When the media clip arrives, the decryption process is initiated and completed by the smartcard.

```
<smil>
 <App name = "Accident No : 6345">
     <Configuration id = "Emergency (EMS)">
             <UserLevelQoS> high </UserLevelQoS>
              <UserFocus> memory </UserFocus>
      </Configuration>
      <Configuration id = "Law Enforcement (911)">
                   <MemUnit mem = "Mbytes"> 5MB </mem>
                   <UserLevelQoS> Average </UserLevelQoS>
                   <UserFocus> Delay </UserFocus>
                   <Delayunit del = "Minutes"> 7 </del>
                   <SLAModel> Conform SLA </SLAModel>
     </Configuration>
     <Configuration id = "Medical Doctor">
             <UserLevelQoS> high </UserLevelQoS>
             <UserFocus> clarity </UserFocus>
             <Clarityunit clar= "pixels/inch"> 200 </clar>
     </Configuration>
</App>
// We will proceeed further only if the QoS thresholds are met
//An alternative here is to use switch with QoS attributes as
// specified in earlier sections.
<body>
  <seq>
          <img   src="Media Clip: Accident No: 6345"/>
          <par>
<Shot1 is encrypted with SymmetricKeyShot1 >
         <shot1>
              <video src="Camera1" dur="45s"/>
               <video src="Camera3" dur="23s"/>
              <video src="Camera2" dur="4s"/>
              <audio src="Camera1   "/>
         <text src = " sensor" />
              </shot1>
          </par>
          <par>
<Shot2 is encrypted with SymmetricKeyShot2 >
         <shot2>
               <video src="Camera3" channel="video2"/></a>
               <audio src="Camera3 audio"/>
              <text src="sensor" dur "8s " channel="text2"/>
              </shot2>
        </par>
Shot3 and all other shots upto ShotN are encrypted with the
respective SymmetricKeyShot (1-N)
             xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
             xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
             xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
</body>
</smil>
```

QoS/Resource Negotiation

Encryption Mechanism

Figure 7: QoS/Resource Negotiation and Encryption Mechanics in SPUTERS

The server at the EHC takes the following steps:

1. Create the keyvector, encrypt with the public key of the client (station) and deliver (unicast) it to the smartcard on the client machine and broadcast the encrypted media clip.

Each client smartcard receiving a keyvector takes the following steps:

1. Decrypt the received keyvector and thereby decrypt the encrypted parts of the media clip with available symmetric decryption keys.

In a broadcast environment in which there is more than one user, there can be a significant transmission delay between media shots due to both the sequential arrival of encrypted shots and the time it takes to decrypt the data. We are currently investigating issues of processing of the data in real time, as well as providing "on-the-fly" encryption that would enable the client to download keys and encrypted media clips with minimal delay. This is non-trivial as the system should also be able to satisfy incident-specific QoS requirements for display.

Our system for traffic surveillance and emergency response uses audio-video services to provide secure three-dimensional stereoscopic multimedia to distributed users from cameras, microphones, and other types of data-collection mechanisms. SPUTERS can be used for traffic analysis and other measurements in crash-prone areas during normal operating conditions and for incident response in case of emergencies. The underlying security model and mechanisms provide explicit support for controlling access to privacy-related data about vehicle occupants, in addition to protecting the integrity of that and other types of collected information. Data, both textual and video, is securely transmitted as SMIL documents that contain role-based access-control information about the contents of the documents. The architecture and design of SPUTERS lends the system well to be both developed with commercial-off-the-shelf products and deployed with minimal additions to the vehicle-highway infrastructure. SPUTERS can provide continuous real-time media services with all specifications for doing so residing in a single document. SPUTERS is extensible, permitting, for example, the addition of the capability to revisit previous scenes of an incident in order to support forensic and legal investigations. An automated assertion system, based on the media information, is also possible with advanced algorithms. Our ongoing research addresses the aforementioned extensions.

COST MODEL COMPARISION

According to our analysis based competitive market survey of integrated products, SPUTERS would a cost-effective choice for mid-level housing locality including high-rises (200 – 1200 units) or a local government. The purchase price of the entire portfolio would be about 110,000. The installation cost is expected to be about 15,000 and the associated roll out costs at about 10,000. The recurring staffing expenses for the organization using the product shall be significantly lower than the traditional models owing to effective customization during the integration process which utilizes existing functionality. The maintenance costs are about half of the cost typically associated with popular COTS models.

MARKETING STRATEGY:

Category	Strategy

Target Market	Mid to Big size HOA based Communities, High-rises (200 – 1200) units and local governments.
Positioning Statement	Build a secures traffic surveillance and roles bases emergency response structure to enable Mid to Big size HOA based Communities, High-rises (200 -1200) units and local governments.
Offering to customers	A reliable cost-effective integrated surveillance and emergency response with very cost effective and customizable portfolios with 24/7 technical support.
Price Strategy	50-60% less than the traditional models offering non-customized services.
Distribution	Implementation, Rollover, Registration and subscriber enrollment for free and maintenance at about 2000 USD a month.
Sales Strategy	Hire a pre-sale team a national account manager and regional account managers. Provide on-site assistance and training,
Service Strategy	Technical Product support, scheduled maintenance and troubleshooting provided free of service for the first 2 years and with a competitive price thereafter for the life of the product.
Promotion Strategy	Make office visits and provide demos to targeted residential communities and pertinent county and city level governmental organizations
Marketing Research	Conduct continuous Research and Development, read governmental reports, private firm reports and keep abreast with the changes and trends in the current surveillance and Emergency response strategies to obtain lower cost effectiveness and efficiency without trading QoS and Security.

KEY DELIVERABLES

The following initial timeline depicts the estimated timing in which surveillance and knowledge base development capabilities and supporting functionality (progressive updatability) and integration with COTS devices will be deployed but does depict all work streams in absolute detail as it is being worked out at during the current time period. A comprehensive, customer –centric plan will actionable detail will be developed during the initiation/ vision phase and the zero and first iterations of the Rational Unified process.

Timeline	Activity	Status
October 2016	Existing recruiting processes and work-flows documented	Completed

	reviewed and approved.	
October 2016 – March 2017	Initiate conceptual design and solution map, including the accountability framework and delegation of authority;	In Progress
March 2017–December 2017	Confirm the strategic direction of the surveillance enterprise architecture and technology solutions	Initiated/In Progress
March 2017–December 2017	SMIL based Knowledge base development for storage and efficient retrieval of multimedia content gathered by external devices.	Preliminary Research
January 2018 – June 2018	Review and refine ensure that the current systems and modules are aligned with the strategic direction, target tools and architecture;	Not Initiated
June 2018 – November 2018	Prepare detailed plans and resource estimates for the high priority phases/projects and obtain approval.	Not Initiated
November 2018 – June 2019	Determine the impact of the conceptual design on the real-time surveillance capabilities;	Not Initiated
November 2018 – June 2019	Prepare conceptual design for Role based Emergency Response	Not Initiated
November 2018 – March 2017	Development and coordinate with the emergency response architecture.	Not Initiated
In Scope – Timeline not decided	Integrate surveillance, Knowledge base and emergency Reponses Architecture.	No Timeline
In Scope – Timeline not decided	Deployment and Test	No Timeline
In Scope – Timeline not decided	Roll Out	No Timeline

PROJECT PLAN

For the SPUTERS development project, milestones and tasks are broadly defined as described below. The following chart outlines the major tasks involved in completing the project and their dependencies, the number and type of resources required for each task, the duration of each task and major milestones involved.

SPECIFICATION /PORTFOLIO VISION PHASE

Task Description	Resources	Duration (days)	Milestone Description
Specification/ and High-level Design (HLD) Phase 1	6	180	Specification complete
Specification/ Phase 2	6	180	
Specification/and HLD for Phase 3	6	180	

Specification/Portfolio Vision and HLD for Phase 4	6	180	
Specification/Portfolio Vision and HLD review of all the systems	12	120	
Incorporate comments from the review and sign off	6	60	

DEVELOPMENT PHASE

Task Description	Resources	Duration (days)	Milestone Description
Phase 1 development and unit testing	5	240	Product design complete
Phase 2 development and unit testing	3	220	
Phase 3 development and unit testing	4	240	
Phase 4 development and unit testing	5	240	
Design review and unit test results review of all the systems	17	50	
Incorporate comments from the design review, iterate on development and/or unit tests	4	50	
Final design review and signoff	4	20	

TESTING AND INTEGRATION

Task Description	**Resources**	**Duration (days)**	**Milestone Description**
Test strategy development and review	4	120	Product testing complete & Production ready
Test cases development and review	8	120	
Test automation platform development and review	4	120	
Automated test case development and review	4	120	
Test case execution (manual and automated) and test results review	12	200	
Overall test results review, re-test / iterate, and signoff	4	60	

PROJECT RESOURCE PLAN

Based on the above project scope and plan, the following resources are required to specify, design, develop, test, integrate and deliver the product.

Resource type and experience level	**Number of resources required**
Project Manager	1
Enterprise Architect	1
Programmer/Analyst, senior level with 5+ years' experience	2
Computer Systems Analyst	2
Business Analysts with 2+ year's experience	4
Software Engineers with 5 year's experience	5
Quality analysts with 2-5 years	5
Total	20

PROJECT ROLES AND RESPONSIBILITIES:

The following table captures the roles and responsibilities of the project resources outlined above and any internal resources assigned to ensure on-time, within-budget execution of the project.

Role	Primary responsibilities	Type of resources	Number of resources
Project manager	Responsible for on-time delivery of the project, meeting the Specification/Portfolio Visions including cost and quality.	Senior project manager	1
Architect & Technical Leads/Senior Programmers	Responsible for architecture, high-level design and Specification/Portfolio Visions of sub-systems & leading teams by motivating, organizing and facilitating of technical tasks and deliverables.	Senior programmer analysts	3
Developers	Write quality code per Specification/Portfolio Vision and design, unit test and deliver to QA.	(1) Software engineers & (2) Programmers	6
Systems Support	Set up and support hardware and software systems (development, test and production environments) required for the project. Develop business and work flows as necessary to include in the product Specification/Portfolio Visions and documentation	Business analysts	5
Testing and QA	Responsible for the development and execution of test strategy and test cases. Responsible release build in a defect-free environment	Quality analysts	5

PROJECT COST:

Based, the overall projected cost for the project works out to be $1,062,900. This includes payroll, facilities, and equipment costs for the development, test and production computing infrastructure.

SUPTERS Itemized Cost

Item	Cost
Payroll Expense	$ 833,300
Licensing fees	$ 105,000
Equipment	$ 63,000
Facilities (rent, utilities)	$ 36,000
Insurance	$ 10,000
Other	$ 15,600
Total	**$ 1,062,900**

PROJECT WORKSITE

The project will be executed at Bytefield Inc's offices at Sterling VA.