White Paper

Revolutionizing Detection of Improvised Explosive Devices Through Real-time, Actionable Information

Table of Contents

1.0 Executive Overview

Analysis of massive amounts of real-time and historic data captured in areas of wartime conflict will revolutionize the impact of intelligence gathering. In a combat environment, speed and precision are key requirements for sifting through the volumes of information available to extract key pieces of relevant and actionable information. Nowhere is the need to turn data into actionable information more pressing than in the current wartime efforts to detect and avoid the horrific impact of Improvised Explosive Devices (IEDs).

As a corporate challenge and directive, SGI has applied its mission critical and engineering expertise, along with a Complex Event Processing engine and the Intel® Itanium® processor, to play an instrumental role in counter-IED (C-IED) operations. By applying technology to automatically and quickly process incoming data and produce a highly accurate search for potential threats, this new solution accelerates access of usable information from a variety of sources by command center and office analysts as well as field personnel for C-IED purposes.

This paper explores how the IED challenge is amplified by the magnitude and velocity of data generated in the theater of operations, and how the application of SGI EventVUE™ real-time visual Complex Event Processing (CEP) solution can turn data into actionable information that is visually represented to a wide range of users. EventVUE helps construct a protective bubble around U.S. and coalition Blue Forces and significantly improves the path to immediate action against this grave enemy threat.

2.0 The Challenge of Persistent Surveillance for Improvised Explosive Devices

IEDs, also known as roadside bombs, have caused about 43% of all the American combat casualties in Iraq, and about 30% of combat casualties in Afghanistan, both killed and wounded.[1] IEDs typically utilize commercial or military explosives, and in many cases the bomb is constructed using whatever materials are available. Triggering methods include a directly connected wire circuit, cell phone, a garage door opener, a radio-controlled toy, or something as simple as air-pressure-activated detonating switches.

The typical IED terrorist cell consists of six to eight people, including a financier, bomb maker, emplacer, triggerman, spotter, and often a cameraman. Being decentralized and opportunistic, they are hard to counter using traditional wartime techniques.

Several options are available to combat IED threats in a pro-active manner. For example, unmanned aerial vehicles (UAVs) and scouts in helicopters can provide successful aerial reconnaissance, moving quicker and providing advanced warning to reconnaissance elements on the ground. Scout elements on the ground can then move forward to confirm or deny information provided by air elements. Another tactic is to place an Observation Post (OP) in cooperative residences near Named-Areas-of-Interest (NAIs). If left in place for several days, these OPs could have some success in observing the enemy attempting to emplace an IED. While such tactics have potential, they also highlight the large human investment and risk required of most C-IED operations.

Persistent surveillance reduces IED effectiveness by interrupting the insurgent chain of IED activities – a tactic known as attacking the network. With a means to automatically and rapidly detect patterns that could indicate the presence of IEDs, military operations could both neutralize threats long before troops move into the area and trace those devices back to their origin, thereby giving the capability to neutralize production and mitigate future threats. However, current persistent surveillance systems suffer from a variety of challenges:

- Coordination and correlation challenges due to disparate data sources and high volume feeds that were never designed to function as a whole. For example, today's systems such as Global Hawk, Predator, and fighter aircraft collect still and full motion video at differing resolutions. The amount of imagery that can be collected today far exceeds the ability of the military or intelligence community to analyze fast enough to apply to C-IED operations.
- In addition to massive amounts of information, persistent surveillance must integrate with multiple networks and monitor access across different security levels and across multiple domains.
- Analysts and commanders must be able to monitor known and developing threats as they maintain control and status across hundreds or thousands of individual troop and convoy movements each day.
- Shortages of well-trained analysts make it difficult to scale up a C-IED operation that uses sophisticated technology.

To date, the computer systems capable of detecting information of interest prove to be highly specialized to specific targets, take a long time to develop, require massive computing power, and have relatively low success rates. As a result, the military continues to rely on human detection. However, human involvement limits the scalability of the solution and introduces error into the process.

1. 1810 deaths as of September 2008 - http://www.icasualties.org/oif/IED.aspx

3.0 SGI Demonstrates a C-IED Solution with EventVUE

SGI has applied its deep understanding of defense applications and its visual computing expertise to a demonstration that automates persistent surveillance for C-IED operations (Figure 1). Based on the EventVUE real-time visual CEP solution, the demonstration exploits existing C4ISR resources, historical information, real-time sensor input and HUMINT reporting to generate location-based alerts in a variety of ways.

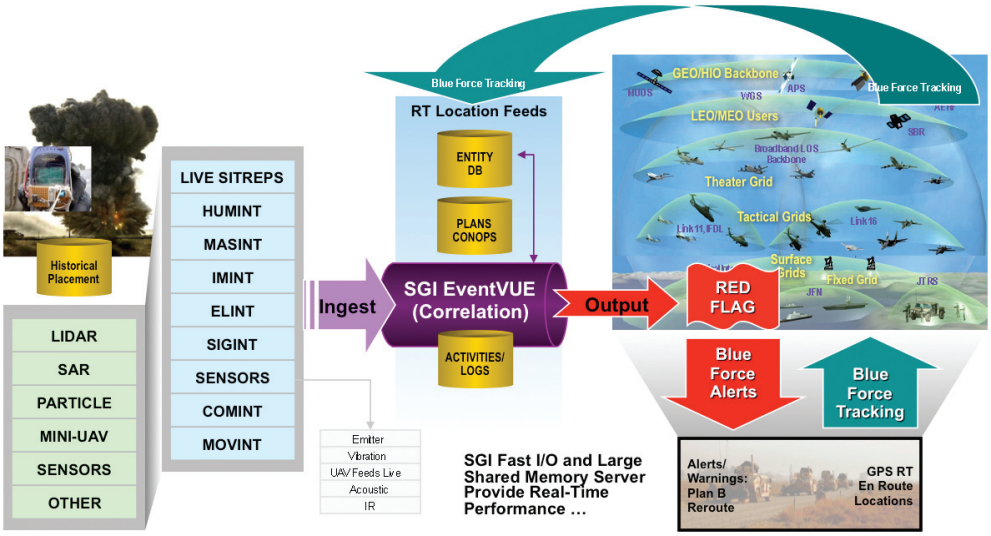

Figure 1: The concept of operations within the demonstration of EventVUE as a solution for C-IED.

Though not deployed in a fully operational environment yet, the SGI demonstration of a solution for C-IED based on CEP techniques is capable of providing rapid, real-time location-based alerting of possible threats related to IED activity in relationship to Blue Force and Coalition Partners. As shown in Figure 1, this demonstration represents how EventVUE can overcome the data collection, analysis, and alerting challenges through the following features:

- Continuous exploitation of disparate, dispersed data sources, including geo-referenced data sources and real-time feeds from tactical and national systems. It can track information from Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signal Intelligence (MASINT), motion detection, CheckPoint Information Services, Social Analysis databases and human identity systems.
- Issuing information and alerts integrated with established and trusted military communications systems (COMMS) as well as common geospatial tools, instant messaging systems, email and even text-to-speech systems for use across voice-based devices (JTRS and other voice-operated radios).
- Comparing incoming data streams with force location information in real time for rapid and continuous correlation of threats vs. actual Blue Force location. It can follow Blue Forces regardless of the planned routes of travel – where the Blue Force goes, so does the roving coverage.
- Identifying a potential threat to provide look-ahead, look-around, and look-behind warning capabilities with geo-referenced alerts and distance to/from threat information.
- Usefulness to mission planners for generating a planned route of travel for Blue Forces before mission commencement.

The demonstration also represents C-IED as a "disruptive technology" that can help increase situational awareness by exploiting social network analysis tools to identify possible players in the IED production chain, including funding, building and placement.

3.1 CEP Architecture Accepts and Processes Many Data Streams

The architecture within the SGI EventVUE real-time visual CEP offers the fastest possible processing of high-volume content for threat assessment, target recognition or other purposes. By using a CEP engine and powerful I/O options, this demonstration shows a practical approach that can be implemented without disruption to existing workflows yet still provides an overview across multiple image sources.

Using the parallel processing capabilities of the CEP engine this example demonstrates how the solution monitors key thresholds in real time to trigger data flow and processing according to pre-determined policies. To accomplish this, it integrates multiple data sources and processing elements in several layers:

- **Physical**: Links various data sources, including live Situational Reports (SITREPS), historical data, sensors, satellites and Unmanned Aerial Vehicles (UAVs)
- **Semantic**: Maps and graphically connects information based on the ontological (or contextual) meaning of each piece of data
- **Geospatial**: Tracks location and movement of assets, threats, and data sources
- **Analytic**: Provides complex analysis via rule-based data correlation for unprecedented visibility and situational awareness of people, infrastructures, communications, facilities and vehicle movement

3.2 Web-based UI For User-Defined Rules

EventVUE employs a powerful web-based UI that simplifies the process of defining rules for processing data, identifying potential threats, and sharing information and alerts. Through the web-based interface, a wide array of end users can create and work with custom real-time information, alert and extraction workflows themselves, thereby reducing demands on full-time systems administrators. As a result, the system can support better decision-making capabilities, decrease reaction times to events and improve filtering of vast amounts of information. Operators and analysts can focus on critical events as opposed to unfiltered streams of random information.

Users can query according to any combination of search criteria. For example, the user may wish to search on a specific geographic area for anything that resembles a target. A search for this shape runs against the data, and returns multiple clips of imagery ("hits") based upon the search criteria. The user can preview, annotate, and route images for action or additional analysis. Each user may have a global view of all databases, so searches triggered by an item of interest in one library can be easily cross-referenced to others. Because all versions of the imagery are linked, the workflow for C-IED maintains the option of routing the high-resolution version of the file when needed.

3.3 Actionable Information Made Visible To Many End Users

For reporting and dissemination, the SGI solution can present search results and automatic alerts visually to a wide variety of end users. The views can be presented at multiple levels in the command structure: a central command view of all the units in the field; through a PC in each unit to provide troops with real-time actionable information during a mission; and a web interface for analysts to review past and current info for planning new convoy routes.

Figure 2 shows a visual demonstration of multiple threat alerts about multiple Blue Force units in a hazardous area. The system presents many dimensions of each threat: geospatial location, proximity to Blue Forces, type of threat (represented by a shape), and alert severity (represented by color). A user can select a threat icon to receive more information on the threat as well as link to additional information from the original data source.

This user interface maximizes all available data and collection disciplines ("INTs") for improved situational awareness and rapid alerting to friendly forces.

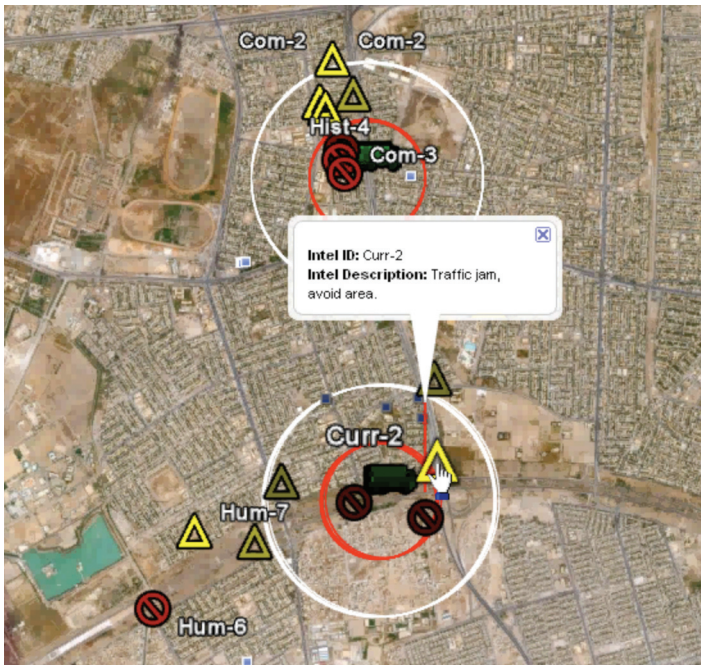

Figure 2 – An example of a visual display of IED-related threat information as presented to a central command monitoring multiple units in the field.

3.4 Commercial Hardware and Software Simplify Deployment

A persistent surveillance solution like the one demonstrated here must be able to deliver information in real time for it to improve decision-making and the deterrence of the IED threat. SGI has implemented this demonstration using its EventVUE real-time visual CEP solution, which integrates a powerful CEP application and high-performance hardware to reduce the processing time – from receipt of source data to a visual alert of relevant information. Off-the-shelf software and hardware speed deployment for real-time, mission-critical data analysis applications, and make it easier to customize real-time, event-driven applications. They also reduce long-term maintenance costs and help make it easier to extend an EventVUE application to meet new and evolving requirements.

EventVUE is built upon the SGI Altix® family of servers based on the highly scalable Intel® Itanium® processor family. In addition to their high performance and enterprise-level reliability, accessibility, and serviceability (RAS), these processors and servers have the ability to handle massive amounts of shared addressable memory (up to 128TB), making them particularly well suited to high-performance analysis of large data sets.

EventVUE real-time visual CEP is non-invasive and well suited to the input-output (I/O) requirements of the C-IED workflow. The solution offers out-of-the box connectors for many types of real-time feeds as well as traditional data sources like databases or image repositories. With unsurpassed I/O capabilities, the Altix platform can scale up to ingest the vast amounts of data being captured around the battlefield. SGI's Peer I/O technology enables high-speed access to SGI's large shared memory for all system components.

Parallel computing capabilities within the EventVUE architecture drastically improve search performance. During this compute-intensive phase of the process, the SGI Altix platform uses SGI Reconfigurable Applications-specific Computing (RASC™) technology to perform shape-characteristic search against all items of interest in parallel. SGI RASC uses hardware acceleration to search models of desired targets within the Shape Files created during the Shape Characterization phase. It can search files local to the Altix server as well as files in storage. Additionally, users can configure EventVUE so content ingested in one location can be browsed, searched and acted upon at other locations, to further match processing needs with available resources.

The EventVUE architecture can scale from a small, field-deployable mobile half-rack configuration to a centralized ingest-and-storage environment capable of absorbing virtually any volume of image sources. SGI provides Storage Arrays, Tape Libraries, and CXFS™ for cross-platform file system support, UPS Solutions, Managed Services and Professional Services for onsite installation, customization and tuning to complete a mission-critical solution.

4.0 Summary

The urgency of countering the grave danger of IEDs provides an ideal example of the need for real-time, actionable information in the battlefield. Persistent surveillance operations must analyze massive amounts of data from many types of sources, as well as historic data, to extract key pieces of relevant and actionable information in real time.

SGI shows how its EventVUE real-time visual CEP solution, using Itanium®-based server technology, can play an instrumental role in C-IED operations. EventVUE can integrate a multitude of data sources, automatically apply user-defined rules to isolate potential threats, and quickly disseminate alerts and information to many types of users. Being based on off-the-shelf technology, moreover, EventVUE helps to reduce the time, investment, and maintenance involved in fielding mission-critical applications, making it easier to derive actionable information for a wide range of government, defense and intelligence operations.

5.0 About SGI

SGI is a leader in high-performance computing. SGI delivers a complete range of high-performance server, storage, and visualization solutions along with industry-leading professional services and support that enable its customers to overcome the challenges of complex data-intensive workflow and accelerate breakthrough discoveries, innovation, and information transformation. SGI helps customers solve their computing challenges, whether it's enhancing the quality of life through drug research, designing and manufacturing safer and more efficient cars and airplanes, studying global climate, providing technologies for homeland security and defense, or helping enterprise manage large data. With offices worldwide, the company is headquartered in Sunnyvale, California, and can be found on the Web at www.sgi.com.

Corporate Office
1140 E. Arques Avenue
Sunnyvale, CA 94085
(408) 524-1980
www.sgi.com

North America +1 800.800.7441
Latin America +55 11.5185.2860
Europe +44 118.912.7500
Japan +81 3.5488.1811
Asia Pacific +61 2.9448.1463

4150 [12/08]

J15400