sgi
INNOVATION FOR RESULTS™

White Paper

Achieving Real-Time Awareness and Actionable Information Within Government, Defense and Intelligence Operational Environments

Table of Contents

1.0 Executive Overview

Government and defense intelligence organizations must collect and process massive amounts of raw data from a wide variety of sources to detect actionable intelligence. Some sources, such as satellites, generate streams of data in real time; others exist in disparate active or historical databases. Threatening events could go undetected if relationships between data elements are not quickly associated and made visible to decision makers. To accomplish their objectives, commanders, analysts and end users need a means to find the key events of interest across all the data that leads to actionable intelligence. These personnel need real-time situational awareness to make the best decisions to support personnel, objectives and assets.

Complex Event Processing (CEP) is an approach that can address and scale up to the challenge of these requirements. It provides a foundation for organizations to quickly design, deploy and scale event-driven applications based on user-defined rules. Using these rules, CEP processes disparate event streams and databases to find time-sensitive information and events as they happen, and alerts users and systems in a variety of ways.

SGI has combined its high-performance computing (HPC) technology and industry-leading experience in visualizing information to deliver a real-time visual CEP solution, based on Altix® servers using the Intel® Itanium® processor for compute-intensive data analysis applications, to provide mission critical response time and alerting within a 3D visual context that is pertinent to the activity. This real-time visual complex event processing platform solves problems related to automated data gathering and analysis across heterogeneous, high velocity data environments by providing unprecedented visibility into information about people, infrastructures, communications, facilities, and military or commercial vehicle movement. The result is a reduced decision cycle and reaction times, with users no longer sifting through massive amounts of data for analysis.

By combining CEP principles and software with proven servers and storage systems, SGI shortens the time to deployment and speed of decisions in a number of government and defense operations that demand real-time, actionable information.

2.0 The Real-Time Challenge for Government, Defense and Intelligence Operations

The sheer scope of government and defense intelligence missions around the world drives an explosion in raw data from a wide variety of sources. Higher resolution satellites, multi-modal sensors, unmanned aerial/underwater vehicles and other input sources are streaming in an ever-increasing volume of data for intelligence collection disciplines such as Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT).

The challenge of rapidly collecting, processing, and presenting these assets as they move through the analytic decision cycle is daunting. Manually gathering data from multiple servers and databases that may reside across diverse security domains in various formats can result in costly delays or missed information. Knowing about a threatening event “after the fact” is of no use.

A number of technologies exist that organizations may apply to this challenge. Designing, deploying and scaling these solutions can be difficult for organizations whose primary mission is supporting governmental priorities, as opposed to IT applications or infrastructure. It is very important to build new solutions on proven technologies to reduce the time and risk of development and increase the opportunity for success.

The government’s greatest ally in a dynamically changing security environment is real-time shared awareness. That is only possible when the technology infrastructure can quickly and easily connect diverse people and systems around the globe. That’s why highly scalable server and storage solutions are necessary to keep data moving and ensure that the right people always have the right information at the right time.

3.0 CEP: A Platform For Persistent Analysis and Alerting

CEP is an emerging method for government and defense organizations to deploy persistent analysis and alerting capabilities applied against vast inbound streams of real-time information.

CEP software provides a foundation for organizations to build and scale next-generation real-time discovery and alert applications. CEP users create “rules of operation” that provide analysis across multiple high volume, high-speed event streams to identity specific events, or even the absence of normally occuring events. Next, it is possible to correlate these events (or lack thereof) against static historical databases or flat files to find changes in patterns, location, or behavior. The CEP system can alert warfighters or first-responders to time-sensitive, mission-critical information, providing the chance for decisive action in the face of critical events as they happen.

CEP applications may initiate proactive actions that execute on these opportunities and events. Alternatively, they may remedy problems via system-to-system interactions, thereby responding to events in real-time based on user defined rules, faster than a human operator who may be overwhelmed at the volumes of data being received.

3.1 The CEP Engine Drives the Application

A CEP engine is the core software that drives CEP applications and typically performs three basic functions:

- Connects to and manages high-speed, high-volume input event streams and data
- Continuously processes and analyzes the event streams using specified logic
- Produces and delivers output information or events based on the processing logic

A CEP engine comprises a scalable server that manages the runtime execution of these functions, a high-level language, and a web-based user interface (UI) for generating rules and defining how alerts will be processed and distributed. An operator uses the web-based UI to describe the relevant data sources, the event of interest based on stream schemas, the desired processing functions and sequencing, and then the functionality of the actual output event stream(s).

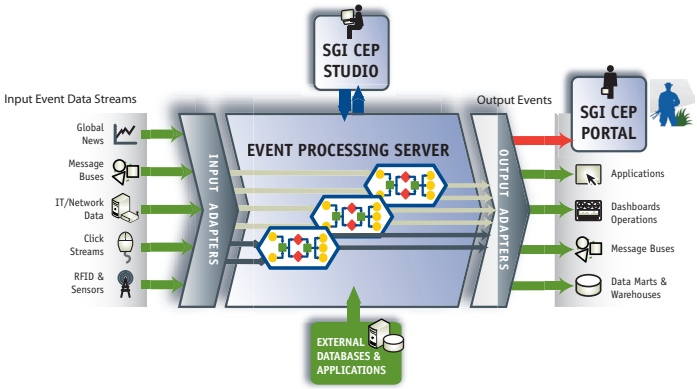

Figure 1: High-level CEP engine architecture

The continuous, in-memory processing model of a CEP engine provides a significant technical advantage for real-time analysis of high-volume event data. For example, a CEP engine running on an Itanium®-based SGI server can process between 400,000 and 500,000 transactions per second. A user can bring multiple CEP engines on-line to cope with increasing data volumes. The CEP engine can, as part of its workflow, also hand off events for further in-stream processing or data transformation (perhaps to application-specific hardware or an external system). Then, specialized algorithms perform their functions and return results to the main stream for further analysis.

This basic architecture can adapt to fulfill a variety of mission-critical roles:

- Continuous exploitation and analysis of data sources to detect critical events
- Rapid and continuous correlation of otherwise disparate data and events
- In-stream detection and alerting when events of interest do occur
- Early warning as rules continuously analyze event streams for known indicators and then issue alerts
- Creation of a detection and workflow environment for system-to-system level interactions

4.0 Moving from CEP to Real-Time Visual CEP

CEP is not a new concept. Specialized applications such as algorithmic trading in capital markets and network management in telecommunications have used CEP techniques to power their architectures for years. However, these applications required extensive custom coding making them very expensive to build, less adaptable to changing requirements, and difficult

to maintain. Also, the processing requirements of the CEP engines were likely to produce a delay between the receipt of data and the generation of alerts to end users. This high cost initially relegated CEP to small groups of specialized users and commercial situations.

SGI introduces a higher performance category of CEP, using off-the-shelf CEP engines and high-performance hardware to dramatically reduce complexity and the cost of building, deploying, and scaling government and defense applications. Through the processing power of the SGI hardware, real-time visual CEP reduces the processing time, from receipt of source data to a visual alert of relevant information, to real-time status. Because the solution is designed to support a web-based operator level interface, a much wider array of end users can create and work with custom real-time information alerting and extraction workflows, eliminating the need for a full-time systems administrator. It delivers better decision-making capabilities, decreases reaction times to events and improves filtering of vast amounts of information to allow operators and analysts to focus on critical events as opposed to unfiltered streams of random information.

Within the solution architecture (Figure 2), SGI introduces a user-friendly approach to defining rules, a powerful platform for executing the rules, and the means to display and share information visually, contextually, and geospatially referenced to multiple parties.

SGI real-time visual Complex Event Processing (CEP)

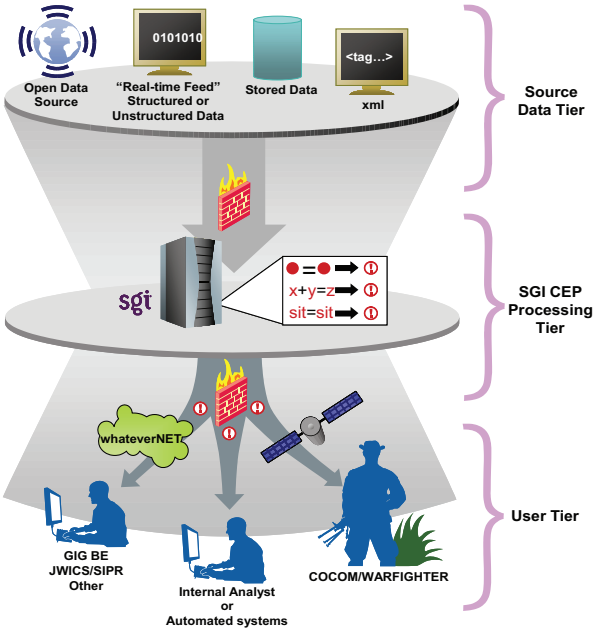

Figure 2: SGI High-Level Real-Time Visual CEP Architecture

4.1 Processing and Analyzing the Information

SGI real-time visual CEP allows users to create simple rule drop-down menus that are related to the specific scenarios encountered by that organization, which will run across all entitled data sources and real-time tactical feeds. The rules are easy to build through a wizard process or via a parameterized template that can be deployed across the operations environment throughout the organization. The underlying platform can scale up to millions of transactions per second, so it can be configured to apply the rules to detect complex intelligence events in real-time. New information such as tips and hunches can also be rapidly correlated against existing data. Concepts such as as event hierarchies, priority, causality and relationships between events based on both temporal and spatial factors can now be analyzed. Imagery from GIS data, for example, can be monitored and gathered from sensors, databases and systems, then analyzed against user-defined criteria and geographic areas of interest and correlated temporally against other data sources. The system also supports internal and external analytics for special use scenarios. In other words, it not only gives an organization the ability to find a needle in a haystack, but it also allows them to find a needle by specific type, shape, color, and manufacturer.

4.2 Sharing the Information

When it detects content of interest, a real-time visual CEP can use a variety of techniques to make information visually apparent to multiple parties at headquarters or in the field. It can propagate alerts across multiple networks, including email, SMS or Web-based alerting to portal interfaces and applications. It also interacts with other downstream targeting or tasking systems. Relevant alerts can support two-way connectivity to databases for updates and set off alerts into situational awareness displays, including existing geospatial tools such as Google Earth™ and ESRI™. The system can also issue IM chat alerts or pass data to link analysis applications like i2 Analyst's Notebook or provide system-to-system alerts to automated targeting and tasking systems. The SGI approach also helps to increase overall situational awareness and promotes a more accurate common operational picture when employed in Command and Control Centers. Customized executive dashboards can be built to provide instant snapshots of what is most important to each decision maker.

4.3 Ease of Deployment Speeds Development

Engine technology enables rapid development of next-generation complex event processing solutions while providing enterprise-class performance, availability and management features for wide-scale deployment and continuous operation in a national security environment. By blending the best of existing enterprise development and deployment features with an innovative high-performance streaming architecture, the solution supports the high-throughput requirements of complex event processing while eliminating the steep learning curve and immaturity typically encountered with new technologies.

The SGI platform is built around the company's 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.

SGI maintains active agreements and partnerships with leading ISVs to extend the solution with CEP-specific software. Using off-the-shelf infrastructure software helps users tailor real-time, event-driven applications faster and at lower cost. It also reduces long-term maintenance costs and helps make it easier to extend an application to meet new and evolving requirements.

This new real-time visual CEP is non-invasive and integrates with existing data sources. 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. Very often organizations deploy a CEP engine interacting with other systems within a broader application architecture, such as the SGI 40G Ingest processor, One-way Guard technologies, Rapid Shape Detection and Full Motion Video management systems. When necessary, SGI also includes customized connectors. To complete the platform, SGI provides Storage Arrays, Tape Libraries, and CXFS™ for cross-platform file system support, UPS Solutions, Managed Services and Professional Services for on-site installation, customization and tuning.

5.0 Powering Mission-Critical Government and Defense Operations

The SGI solution is a general-purpose platform with all the tools needed to apply it to real-time processing and analysis across a wide variety of mission-critical operations. In such operations, threatening events may go undetected if relationships between data elements are not identified. Manually gathering data from multiple servers and databases that may reside across diverse security domains in various formats can result in costly delays or missed information. A real-time visual CEP solves those problems by delivering automated data gathering across heterogeneous, high velocity data environments to provide unprecedented visibility into information about people, infrastructures, communications, facilities, military and commercial vehicle movement and communication networks. The result is reduced decision and reaction cycle times, with users no longer having to sift through massive amounts of data for analysis, providing a true MULTI-INT correlation and alerting capability. Following are a number of government and defense operations suited for this new solution.

5.1 Large Data: Tactical Insight from "Big Data

The U.S. military relies on a broad range of intelligence, surveillance, and reconnaissance (ISR) systems to give warfighters the data required for successful operations. Today, remote sensors work at a higher resolution and across multiple spectrums. This means that the amount of data being generated has grown tremendously, requiring new technologies to retrieve, store, move, and make sense of it. At the same time, government statutes mandate better integration of ISR capabilities among the intelligence community (Director of National Intelligence (DNI) Horizontal Integration initiative).

At the Naval Research Laboratory (NRL), these challenges are being overcome with the Large Data Joint Capability Technology Demonstration (LD JCTD) project. NRL's team of scientists and engineers has architected revolutionary high-speed data acquisition, federated storage, retrieval, and access systems that enable military planners to effectively utilize the mountain of data being created from an ISR, making the information rapidly accessible from their desktops regardless of where the information is physically stored.

SGI supports LD JCTD with an array of Altix® servers as a high-performance clustered file system. In a CEP-like architecture, the SGI computer servers, based on the Intel® Itanium® processor, carry out image processing, data management, and automated indexing functions. These and other SGI products allow this program to continue to overcome bottlenecks and achieve greater throughput and scalability while reducing administration, maintenance costs, physical footprint, and power consumption.

NRL's LD JCTD project proves that it is possible to greatly advance ISR capabilities through a CEP approach. Today, large data sets are successfully being moved in real-time between Korea and Virginia LD JCTD sites. The robust, reliable, and scalable storage, computing, and distribution network has been built across geographically dispersed sites interconnected by multiple, high-speed, low-latency data links. Images from the field are streamed in real time to a data center at rates that can exceed 1 terabyte (TB) per hour per sensor. Individual file sizes span to several terabytes, and multiple images are often digitally *stitched* together to provide a larger, coherent view of an area, and to incorporate multi-spectral data such as visible light, infrared, and radar. With potentially dozens or hundreds of sensors streaming data in any particular theatre, the amount of raw data that can be ingested, stored, processed, and shared can total petabytes (PB) or exabytes (EB).

The ongoing collaborative work that has gone into NRL's LD JCTD project has made it possible for today's intelligence community to handle increasing volumes of data, maintain it across a global network, and achieve low latency for real-time access.

5.2 Defined Area Monitoring

The use of CEP technology can improve detection of events such as ships, aircraft and convoys that are entering certain geographical areas such as harbors, airspace, and cities, and then alert users in a variety of ways.

In one scenario, an SGI system detects aircraft movement and, using predefined rules, notifies end users that this aircraft is of interest and will depict its location geospatially. Based on this alert, the system is able to provide additional information and suggest actions that should be taken with this type of aircraft: it may send alerts to other users or other systems (automatically); it may retrieve and display the country of origin, registration or flight plan on file for the aircraft.

Monitoring shipping vessel traffic in harbors or specific shipping lanes requires fast processing of data from many information sources such as radar, automatic identification systems, and Geographic Information Systems (GIS). When a new ship enters an area of interest, it is identified by one or more of these detection systems and its location is plotted to the GIS. Often in very busy ports, GIS screens become crowded, making them difficult to read and understand.

The new system may assist users by applying application-specific rules such as the following:

> Alert users of a ship that enters an area of interest, originating from a particular country, with a crew member that is on a watch list, and carrying a potentially dangerous material such as ammonium nitrate (as shown in its shipping manifest), display that ship's location and direction plot in neon orange on the area of interest map.

Commanders can now see a much cleaner version of the map with only the potential-risk vessels highlighted in neon orange plots. A neutral color indicates ships with cargo that is neutral as well as a cargo or crew not of interest. This makes actionable intelligence immediately visual, providing analysts queues to rapidly drill down on ships that may pose a threat or be engaged in illicit activities.

5.3 COCOM Situational Awareness

For military operations such as combat missions, search and rescue, etc., geospatial awareness is critical to the success of the mission by providing actionable intelligence. The SGI solution can provide the specific operational information commanders need to observe, orient, communicate and act decisively from headquarters to warfighter.

In one possible scenario, a commander is alerted that one of their personnel units is missing due to not making a radio checkpoint. The real-time visual CEP system can visually display that critical event as well as correlate the information with other key details such as the unit's last known position, threat locations, weather info, and the proximity of other allied assets that are available to respond for a search and rescue. When changes occur to any aspect of the situation related to the search and rescue (such as changes to threat position or weather), the commander can adjust tactics in real time based on immediate alerts that are overlaid onto the mission planning board.
Users have control over the rules and priorities for alerts and scenarios, as shown in this example:

> Only alert me if threat conditions enter Area A or Sector B more than twice in the next 48 hours. If weapons 'XYZ' are verified to be in use, then send a high-priority alert to the operations center GIS; otherwise, send a medium priority alert to the operations center real-time Pixel Fusion feed for 3D contextual display of the search and rescue arena.

By defining and sending priority alerts, combatant commanders have much better knowledge and control of their battle space by being able to respond to events in priority order. In effect, the solution acts as an expert system offering a step-by-step plan based on rules and priorities that they set.

5.4 Real-Time Threat Warnings

The massive amount of still imagery and full motion video available within areas of conflict has revolutionized intelligence gathering. In a wartime environment, speed and precision are key requirements for sifting through the volume of information to extract the key pieces of relevant information. This problem is nowhere more prevalent than with the need to detect Improvised Explosive Devices (IED).

To provide a real-time, fixed, and mobile early warning ahead and around “Blue Force” in relation to possible or confirmed IED threats, a counter IED solution must collect and analyze data from multiple real-time intelligence databases, historical IED placement databases, HUMINT reporting, and other geospatially referenced “INTs” (SIGINT, IMINT, MASINT) sensors.
SGI delivers a comprehensive platform that exploits existing Blue Force Tracking (BFT) resources and, in real-time, correlates friendly force location against geospatially indexed threats. To make actionable intelligence visual to a variety of end users, the system can deliver immediate alerts and warnings via SGI Visualization Systems, email, heads-up display, IM chat, JTRS radio (using text-to-speech converter), and other customized means of communications

Additionally, the capability could be expanded to ingest content from multiple image sources into an aggregated search environment without disruption to the infrastructure or mission of each source. Thus, users cannot only rapidly search content almost immediately after it is ingested, but also correlate it with other views of the same event or area of interest.

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. Metadata is automatically and quickly generated for vast amounts of content, enabling a highly accurate search for any object related to the IED problem. This will vastly speed up the process of getting usable information to analysts and the field from incoming feeds.

6.0 Summary

CEP as a category has a number of advantages in meeting event-processing requirements in government and defense operations. The CEP architecture is designed to collect large amounts of information from disparate sources, process and analyze the information to look for events of interest, and then share that information with users and other applications across a variety of media. To date, deploying CEP has required significant time and resources to customize the technology to specific uses.

With a dedicated focus on the government and defense programs, SGI specializes in delivering solutions that contribute to speed, agility, and flexibility. SGI server and storage solutions are uniquely designed to:

- Enhance the quality of information
- Produce shared situational awareness
- Provide critical information and ensure knowledge superiority
- Reduce time to act and react

With the real-time visual CEP, SGI introduces a higher level of performance to meet the real-time requirements of mission-critical operations. It’s a flexible platform that can be quickly adapted and appropriately scaled to the organizational and user requirements in government and defense operations that span multiple input streams, data processing and analysis, and information sharing, supporting the people and programs that require immediate decisions.

7.0 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

© 2008 SGI. All rights reserved. SGI and Altix are trademarks or registered trademarks of Silicon Graphics, Inc. in the United States and/or other countries worldwide. Intel and Xeon are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Linux is a registered trademark of Linus Torvalds in several countries. UNIX is a registered trademark of The Open Group in the U.S. and other countries. All other trademarks mentioned are the property of their respective owners.

4128 [10.17.2008]

J15386