

## **Complex Event Processing – An Emerging Paradigm in Business Intelligence, Security and Monitoring and Control**

Complex Event Processing (CEP) is a technology which has been used for many years in the Aerospace and Defence Industry for Situational Awareness and Data Fusion modules in Command, Control, Communications, Computing and Intelligence Systems (aka C4I).

Currently CEP is being rediscovered as a foundation for new class of extremely effective Business Intelligence, Security and System/Network/SCADA Monitoring solutions in industries like Financial Services, Telecommunications, Oil and Gas, Manufacturing, Logistics etc.

The increasing connectivity and processing power of the modern IT and Telecom technologies lead to increasing speed and volume of the dataflow available to the organisations. By using CEP solutions companies can gain competitive advantage by achieving real-time situational awareness and tapping the information value that is hidden within the streams of real-time event data that are coming from a variety of sources such as enterprise applications, financial transactions, sensor networks and supply chains.

CEP solutions monitor fast moving data streams and leverage the information to achieve operational insight in the areas of Business Intelligence, Security and Monitoring of Systems/Networks/SCADA. CEP can monitor events in real-time, seeking out the patterns and relationships within the data that have meaning to the organization. They can identify important events, event patterns and situations that signal new opportunities, critical threats, changing conditions, or other material factors that will impact the organization. CEP solutions can give organizations increased capacity for competitive action and improve their level of security.

### **CEP Products**

There are several levels of CEP functionality depending on the complexity of event processing and inference.

Since CEP (as it is used in business applications) can trace its origins in the Aerospace and Defence Industry it may be appropriate to use the JDL Data Fusion functional model to define the various levels of CEP processing. JDL stands for Joint Directors of Laboratories (JDL) of the US Department of Defence.

The JDL functional model specifies 4 levels of Data Fusion functionality with increasing complexity of data processing and inference of high-level information. For the purposes CEP any references to Data Fusion in the JDL model will be replaced with CEP and any references to sensor data and signals with Events.

CEP Level 1 (derived from JDL Level 1) - Event pre-processing, refinement and adaptation. Event sorting and correlation into groups with each group representing data related to a higher-level event.

CEP Level 2 (derived from JDL Level 2) – Fusing spatial (here spatial doesn't necessary mean geographical) and temporal relationships between groups of events to infer complex abstract patterns. The product from this level is called Situational Awareness.

CEP Level 3 (derived from JDL Level 3) performs predictive analysis of the results from Level 2 to proactively identify threats and opportunities.

CEP Level 4 (derived from JDL Level 4) performs process refinement, which is an ongoing monitoring and assessment of the CEP process to refine the process itself and to regulate the acquisition of data to achieve optimal results. Level 4 interacts with each of the other levels.

In business applications of CEP, Level 3 and 4 can also be used for automatic control in business process management solutions.

Most of the current, widely spread CEP products offer capabilities corresponding to CEP Level 1 and to some extent Level 2. They are based on discrete rules for pattern matching. The rules are written in Event Processing Language (EPL) and then executed by a Pattern Matching Engine directly on the stream of events flowing through it in real-time. The power of expression and processing offered by EPL and Pattern Matching Engines is sufficient for CEP Level 1 but not necessarily for complex inference and prediction problems arising at Level 2 and 3.

There is also an emerging class of CEP products based on techniques such as Bayesian Inference that firmly occupy CEP Level 2 and there is intensive R&D underway to provide the predictive capabilities required at Level 3.

In general if the problem can be solved with a list of discrete rules then the problem is not a good candidate for the latter category of CEP products, which is more appropriate for ambiguous and noisy problem domains and CEP Level 2 and 3.

CEP products based on techniques such as Bayesian Inference can be used as a complementary CEP engine by organisations requiring CEP solutions covering Level 1, 2 and 3. If there is a need for CEP solutions focused mainly on Level 2 and 3, they can be used as a standalone CEP engine.

## **CEP Product Vendors**

The vendors offering CEP products can be divided into two groups based on the CEP functionality described above.

Vendors of Rule-Based Inference Products – [Progress Apama](#), [StreamBase](#), [Coral 8](#) and [Esper](#)

Vendors of Bayesian Inference Products – [Inference Machines](#)

## **CEP Professional Services**

CEP is still a young industry and consists mainly of product vendors offering

professional services specialised in delivering CEP solutions based on their own CEP products.

There are emerging business opportunities for vendor-independent professional services organisations specialised in CEP solutions leveraging key advantages such as:

- Objectivity when helping clients navigate the CEP industry and advising on product selection.
- Service portfolio which complements CEP with EAI, Security, Real-Time Enterprise, NGN Telecom Solutions etc.
- Unrivalled experience with large-scale CEP, EAI, Security and Real-Time Enterprise projects in industries like Financial Services, Telecoms, Energy and Aerospace and Defence.
- PoC and Training Centre designed from the ground up to test and assess the capabilities of all leading CEP products, refine our CEP Solution Delivery methodologies and train our staff.
- Unmatched experience with both Rule-Based Inference CEP products and CEP Products based on Bayesian Inference Algorithms.

[iSec Consulting](#) is one example of professional services organisation specialised in turn-key CEP solutions.

## **Design and Delivery Methodology for Turn-Key CEP Solutions**

The following is a high-level description of methodology for designing and delivering turn-key CEP solutions.

- Define the problem – target business domain and complex events and situations of interest.
- Identify sources of events
- Identify the low-level event types representing the problem domain.
- Design event objects
- Design event hierarchies and causal models reflecting the target domain
- Specify the requirements of the CEP project
- Select CEP product meeting the requirements of the project
- Instrument the target event sources to produce the required event objects
- Adapt the CEP engine interfaces to the designed event objects and the organisation's IT and Telecom infrastructure
- Develop Pattern Matching Rules in the Event Processing Language (EPL) supported by the selected CEP product
- This step is valid only for CEP Products based on Bayesian Inference Techniques - Design a hierarchy of learning and memory nodes reflecting the problem domain. To solve problems from different domains and of different types the product is trained rather than programmed. The programmer prepares the Event data for the product and then trains it. The trained CEP product can then analyze new Events and act on them.
- Use Event Simulation Tools capable of simulating event types and causal models to test the inference capabilities of the CEP solution
- Use Event Simulation Tools to test the throughput of the CEP solution

## **CEP Solution Scenarios**

Financial Services - business intelligence, security, fraud prevention, money laundering prevention, algorithmic trading, monitoring, prediction and detection of system status of complex distributed applications and networks

Telecommunications - business intelligence, security, QoS, Revenue Assurance, monitoring, prediction and detection of system state patterns in complex networks.

Energy, Oil and Gas - monitoring and detection of system state patterns and failures in complex pipeline systems and power transmission and distribution networks, algorithmic trading

Utilities - monitoring, prediction and detection of system state patterns and failures in complex SCADA systems.

Manufacturing - plant floor analytics and monitoring, prediction and detection of system state patterns and failures in complex SCADA systems, RFID solutions.

Logistics - supply chain management, RFID solutions.

Automotive Industry - vehicle management systems (embedded or telematics-based).

Aerospace and Defence - situational awareness and data fusion modules for C4I systems.

### **Author:**

Evo Eftimov  
iSec Consulting Ltd [www.isecc.com](http://www.isecc.com)  
Mob: +44 (0) 7900847162  
Email: [evo.eftimov@isecc.com](mailto:evo.eftimov@isecc.com)