



Event-based Middleware & Solutions group

Complex Event Processing

Dr. Asaf Adi

Manager, Event-based Middleware & Solutions

IBM Haifa Labs

adi@il.ibm.com

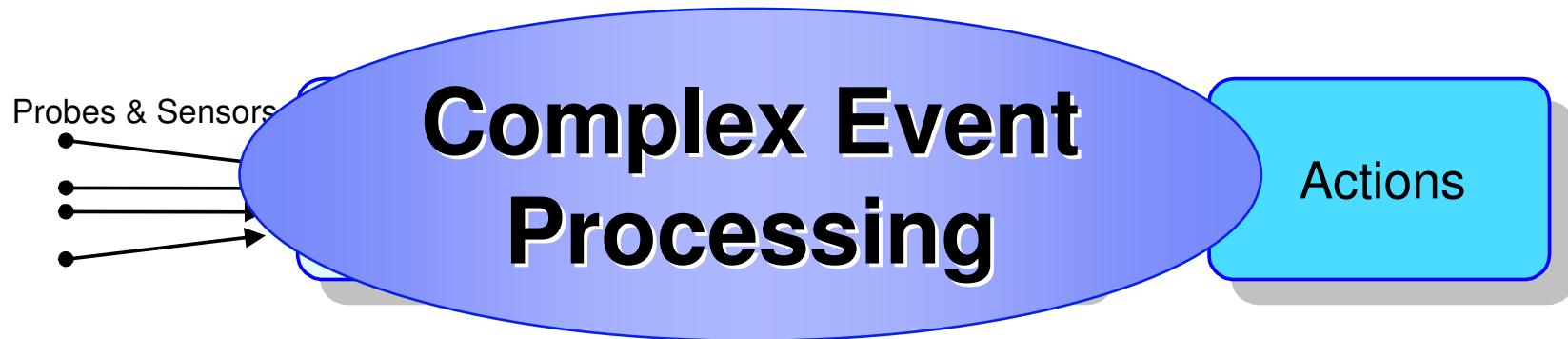
Complex Event Processing

"The fewer data needed, the better the information. And an overload of information, that is, anything much beyond what is truly needed, leads to information blackout. It does not enrich, but impoverishes"

Peter F. Drucker

Founding father of the study of management

Complex Event Processing is about getting better information, in real time.



Action triggered not by a **single event**, but by a **complex composition of events, happening at different times, and within different contexts**



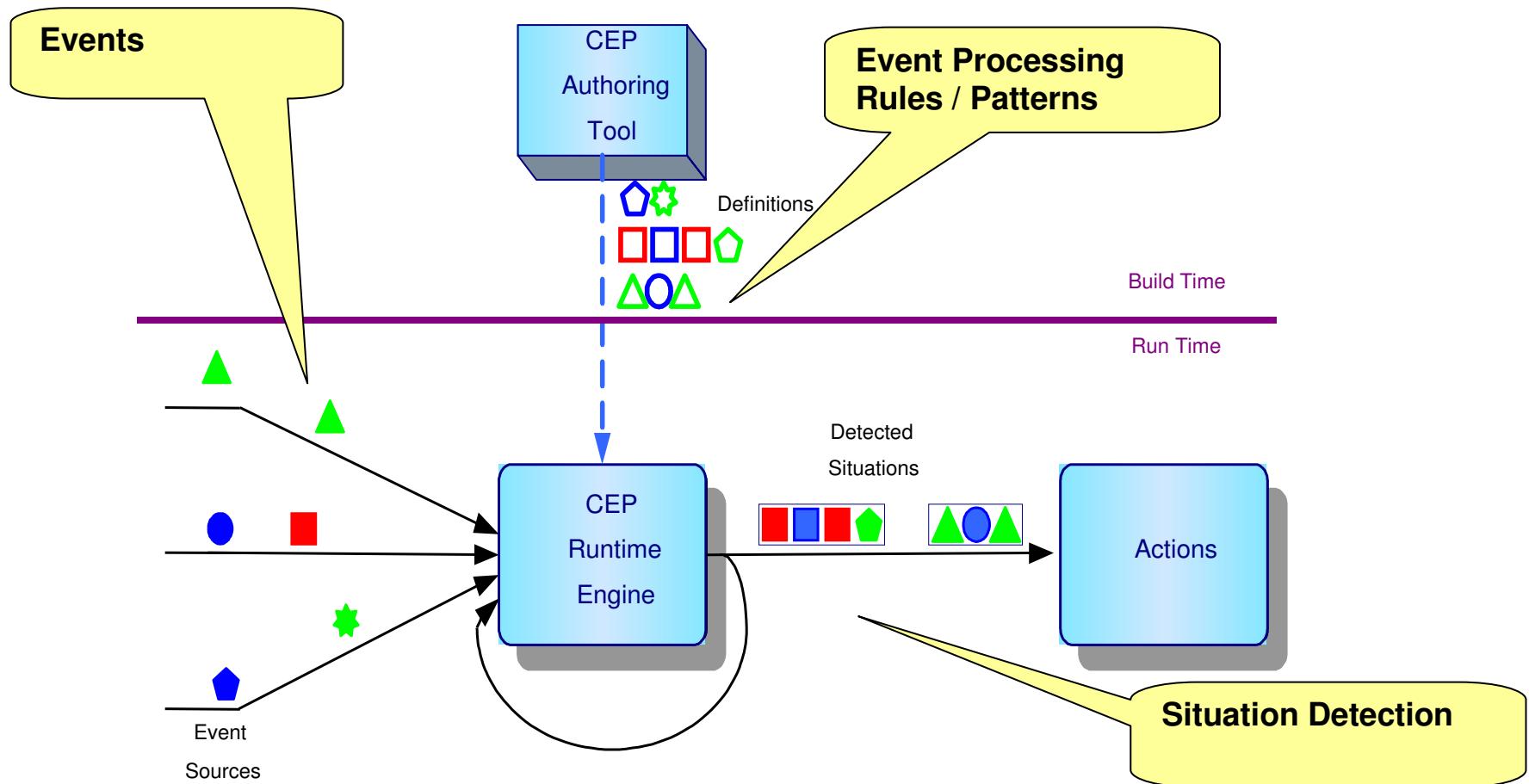
Complex Event Processing (CEP)

CEP is an approach that identifies data and application traffic as "**events**" of importance, correlates these events to reveal predefined **patterns**, and reacts to them by generating "**actions**" to systems, people and devices.

CEP is based on the observation that in many cases actions are triggered not by a single event, but by a complex composition of events, happening at different times, and within different contexts

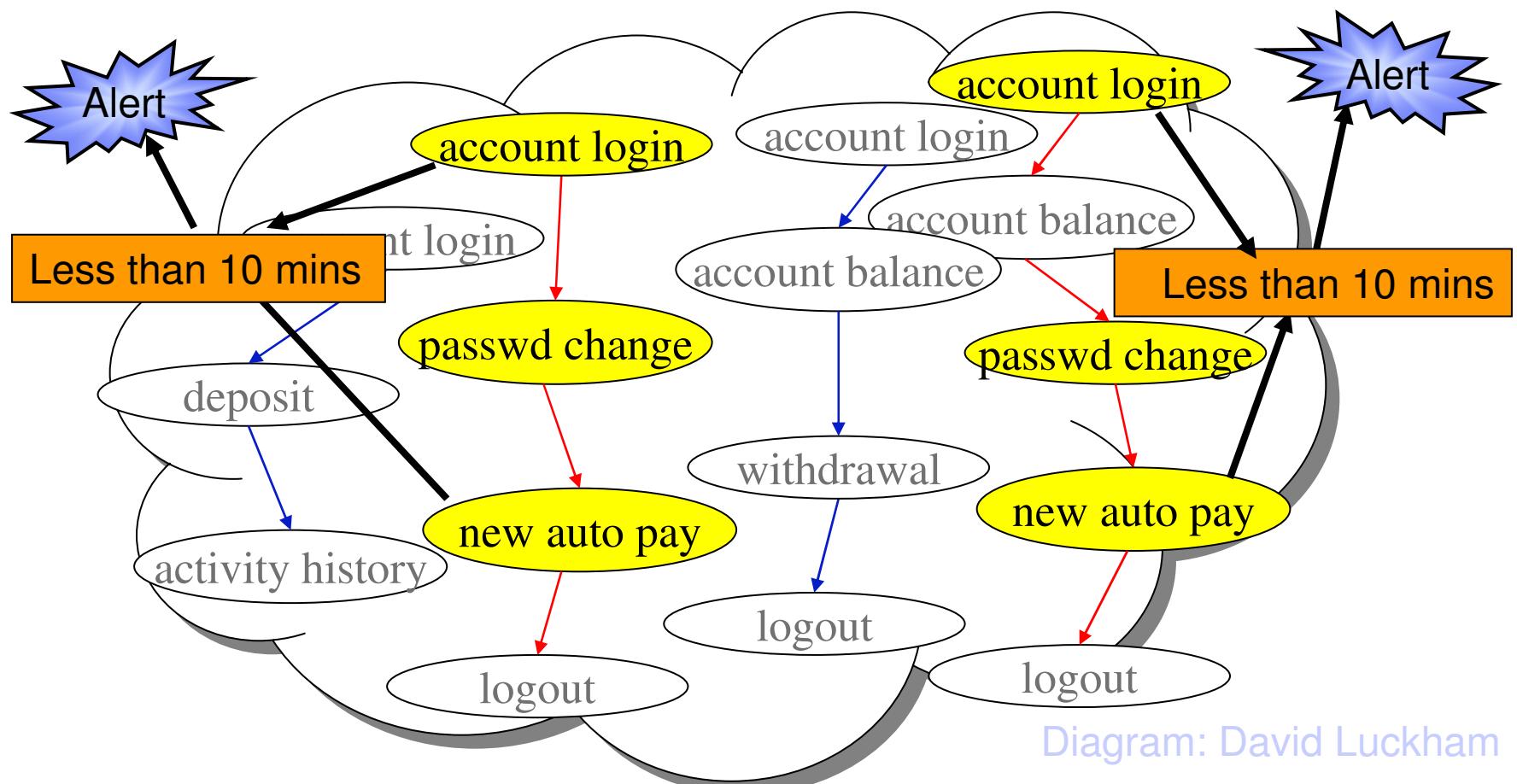
CEP – From Single Event to Situations

Website : http://www.haifa.il.ibm.com/dept/services/soms_ebs.html



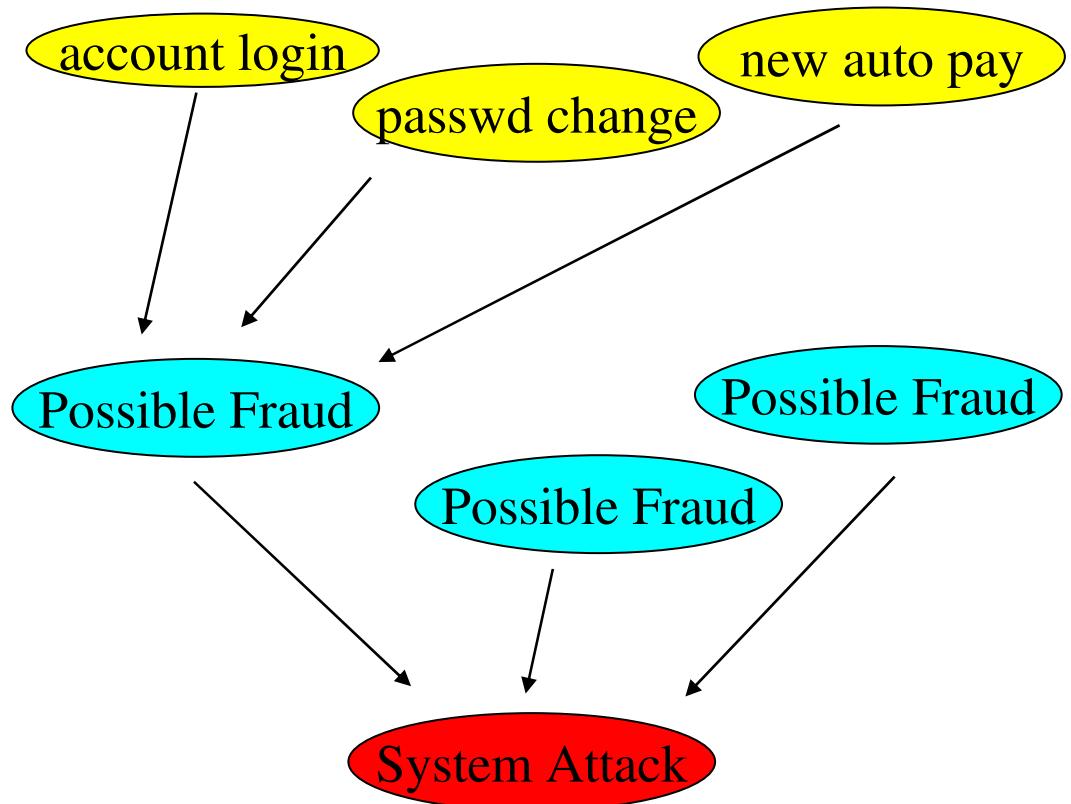
The Concept of Complex Event Processing (CEP)

CEP Example: Detecting abnormal activity in the event cloud in an on-line banking website



Event Hierarchy

- Real events summarize into virtual events which in turn can form an event hierarchy....
 - Login event, password change event, new payment event (real events)
 - Alert to consumer that perhaps account is compromised (virtual event)
 - Multiple of these Alerts might indicate a system attack (virtual event)



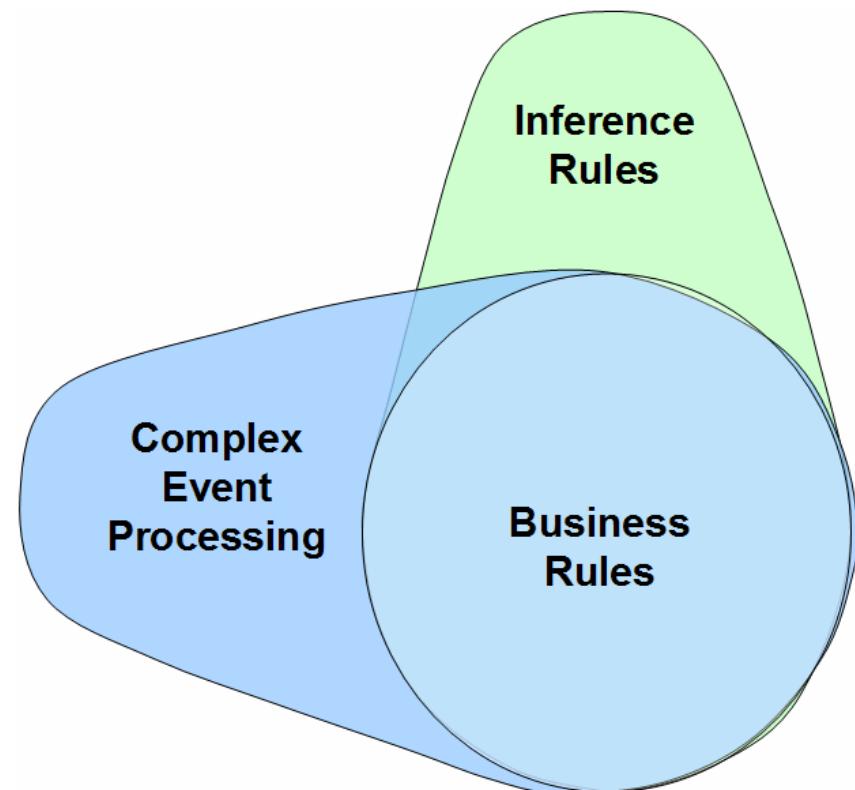


Complex Event Processing examples

- **Regulatory constraints**
 - report on a bulk buy transaction that is performed less than one day after a bulk sell.
- **Fraud detection**
 - Report when two credit card purchases are performed within an hour at a distance greater than 300 km.
- **Aggregation**
 - Report at a set time (e.g. the end of a business day) the number of purchase requests that were processed, their total dollar amount and the average dollar amount.
- **CRM**
 - Alert if three orders from the same platinum customer were rejected for the same reason during a 24-hour period
 - Alert if an order was sent for processing and no response was received within the time specified by the SLA
- **Intelligent Routing**
 - Route a trade message through SWIFT. If ACK is not received within 10 minutes and the trade \$ value is higher than threshold try again. If ACK is not received after 3 attempts use telex.

CEP can express rules that cannot be defined intuitively in other paradigms (In addition to traditional if - then business rules)

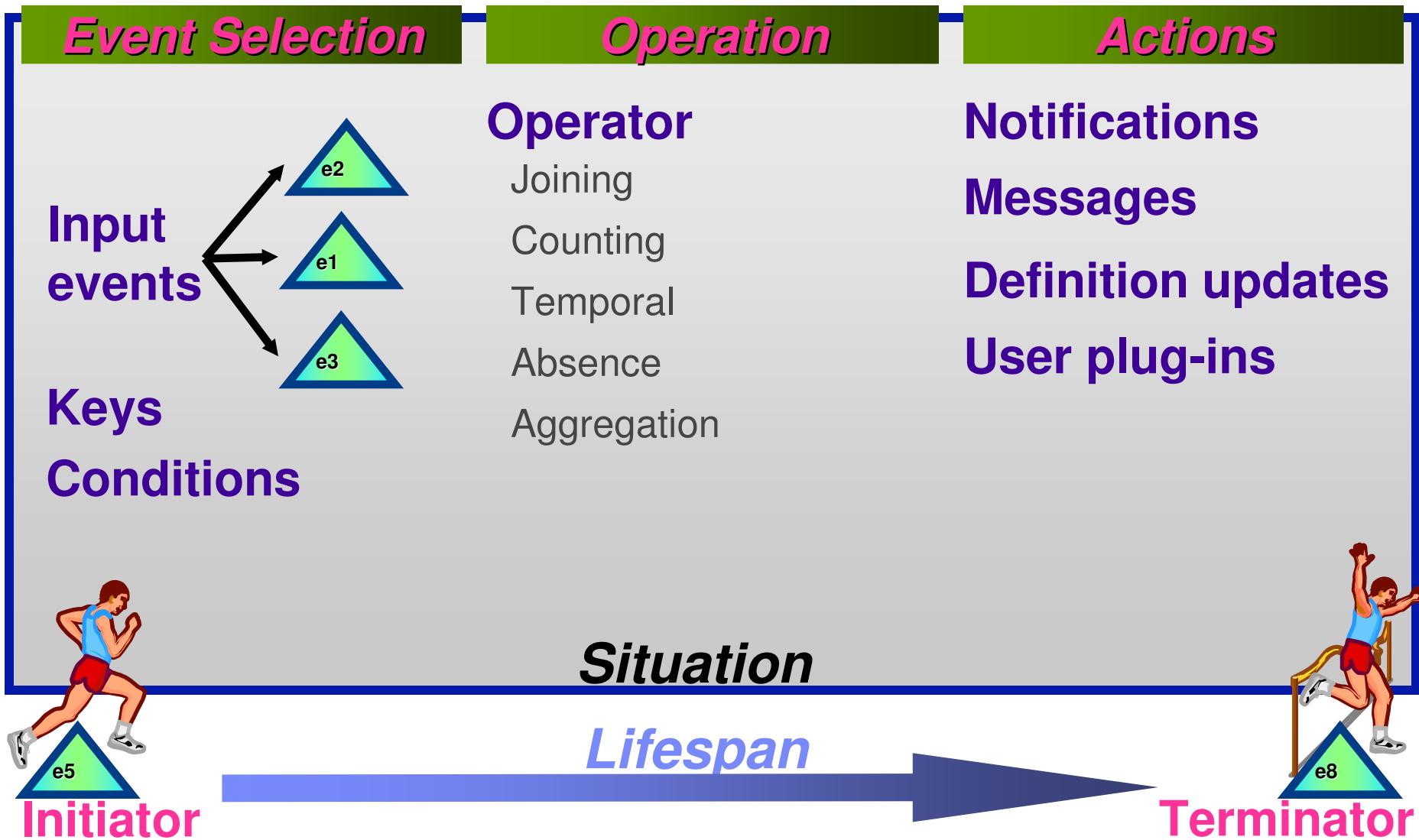
- Event Logic Patterns
 - Events arriving in a certain sequence
 - Counting of events
 - Absence of events
 - ...
- Semantic context awareness
 - Events from the same customer
 - Events from the same account
 - Events with the same time stamp
 - ...
- Built-In Temporal awareness
 - Events accrued within a certain (moving) time frame
 - Timeouts



Typical Usage Scenarios

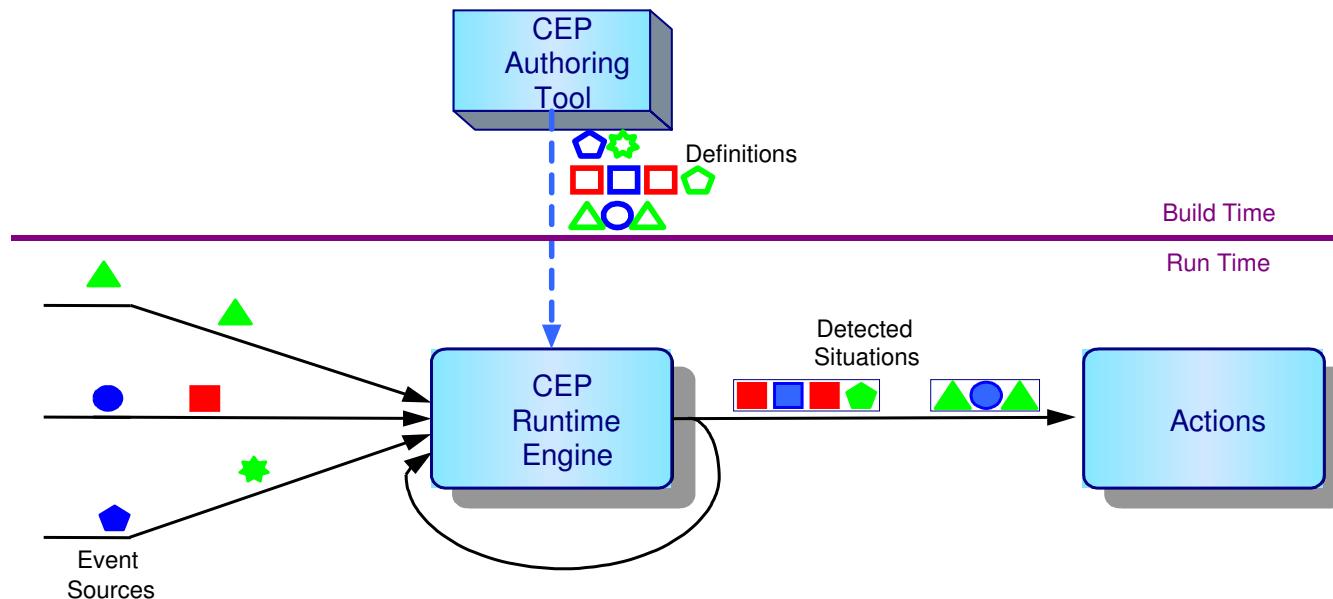
- Business Activity Monitoring (observation)
 - Exception detection
 - Fraud detection
 - Alert notification
 - Triggering of actions
- Rule-based routing
 - Content and Context-based routing
 - Exception handling
- Process invocation
 - Using CEP situation detection to trigger actions

CEP Language – the Situation Concept



The Complex Event Processing rule engine

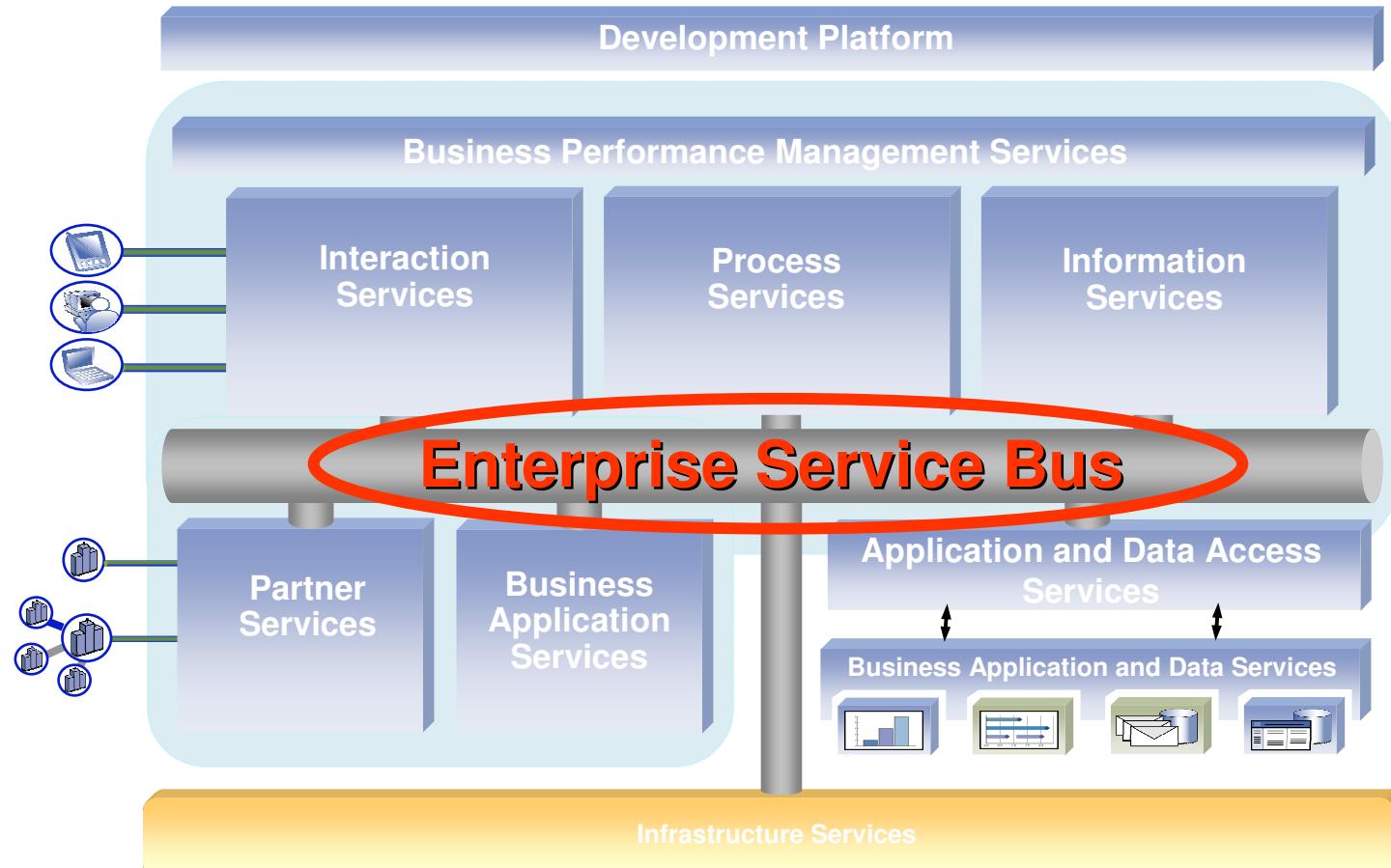
- Eclipse based development environment
 - Wizard-guided process – no programming skills are required
 - Expressive language to define business rules
 - Complex and intricate rules and conditions can be easily implemented
- A runtime engine
 - Detects situations – conditions based on a combination of events
 - Pure Java implementation – multi platform
 - Runtime definition update (Hot deployment)
 - Optimized for event processing



The Complex Event Processing rule engine

- Complex Event Processing combines the following features:
 - *Situations* – conditions defined based on the event history, expanding traditional rules
 - *Temporal awareness* – define the time frame that is relevant to the situation
 - *Expressive power* – rich, high level, language for the definition of situations.
 - *Business level modeling* - Eclipse based development environment
- Complex Event Processing is available as:
 - A Websphere Message Broker product extension
 - WBI Express business rules
 - GBS assets:
 - CEP for Underwriting
 - Insurance Service Hub
 - Embedded in business partners' products (Bristol, Syncron)
- CEP Implementations:
 - Standalone Java Application
 - J2EE Application

Where CEP fits in the WebSphere Business Integration Reference Architecture



The role of CEP in the ESB

Transport Services

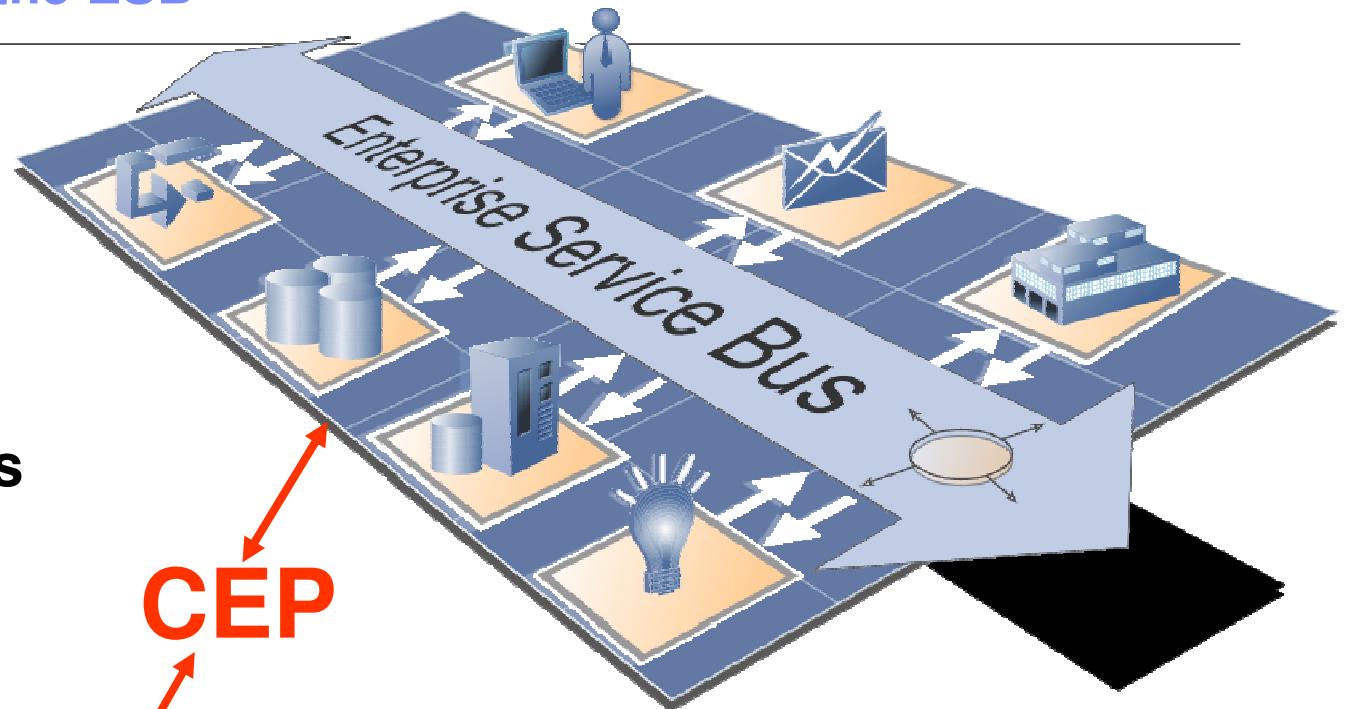
- Assured Delivery
- Secure Delivery
- Transactional Delivery
- Manageable Delivery
- Qualities of Services

Mediation Services

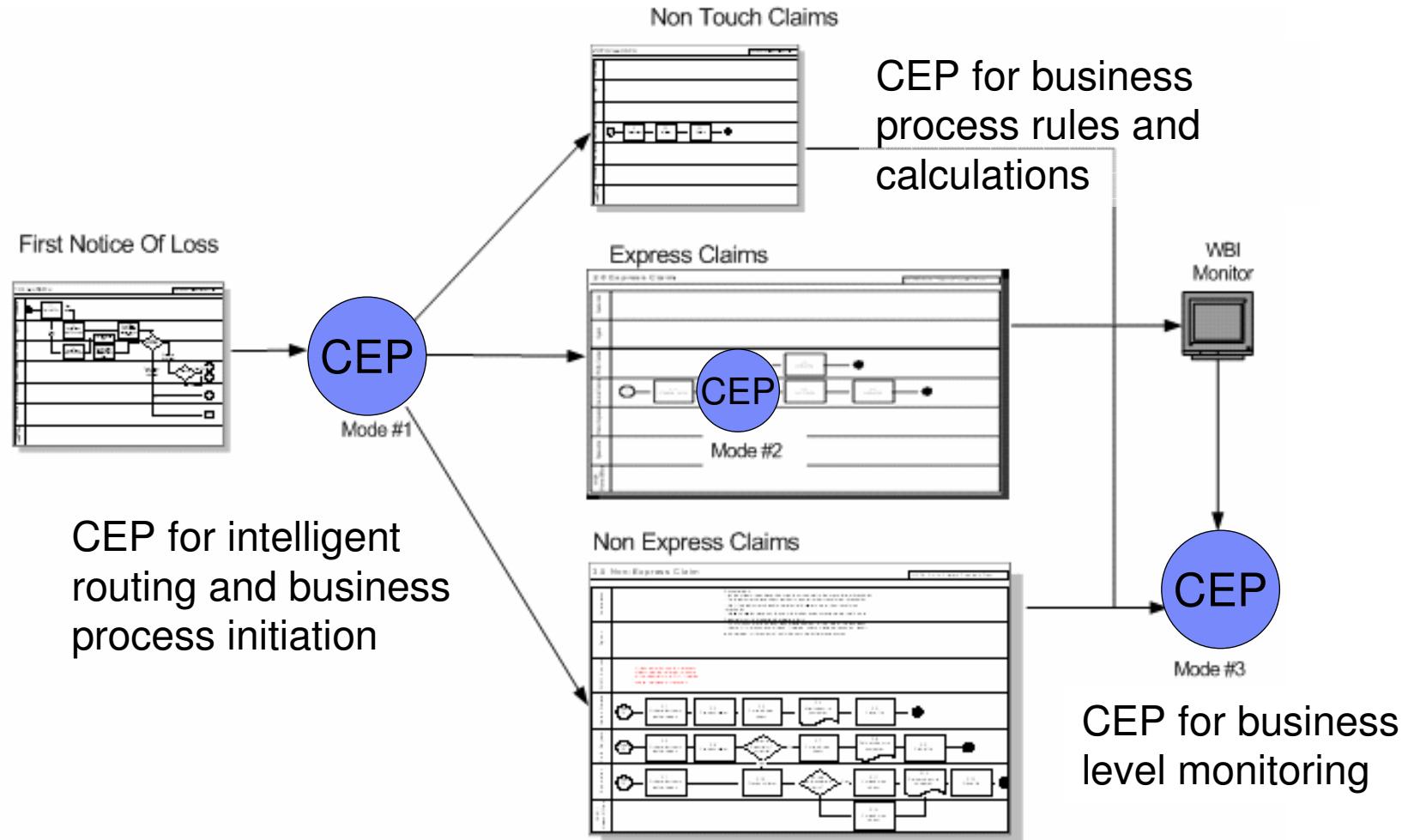
- Routing
- Transformation
- Augmentation
- Customization

Event Services

- Event Handling
- Event Detection
- Event Triggering
- Complex Event Processing



CEP is enhancing BPM capabilities



CEP Value Proposition

- Ability to detect real time threats and opportunities
- Have consistent behavior across the enterprise (no longer Manual or Semi automatic event processing)
- Add Business agility and quick reaction for changing requirements/ regulations
- Enabling flexible, state of the art enterprise architectures (SOA, EDA)



Summary

- CEP is a robust and efficient event driven rule engine
 - Introduces the concept of Complex Events
 - Supports NFR like runtime updates (Hot Deployment) high availability, recovery, scalability, flexibility, and more.
- Allows development of event driven application by non-programmers
 - Wizard-guided tooling
 - Templates
 - Expressive language



Team's Website

- External - http://www.haifa.il.ibm.com/dept/services/soms_ebs.html
- Internal - http://w3.haifa.ibm.com/dept/services/soms_es.html



Event-based Middleware & Solutions group

CEP Case Study





Case study – Banking Alert System

- In this case study, a bank wants to provide his customers personalized information on their activities including: account activities, stock market activities, currency exchange rates and more

- The bank would like that the customer will be able to customize these alerts (e.g. set thresholds), define the deliver mechanism (e.g. mail, SMS) and the frequency in which the alerts will be provided (e.g. during business hours immediately, otherwise in the next business day)

- CEP rules are used for identifying such alerts and for deciding on the delivery mechanism.



Banking alert System – Sample Rules

- Notify when there has been a withdrawal of a total of \$X from an account within Z hours. (X and Z are definable parameters at subscription to the alert)
- Notify when there were at least X ATM withdrawals of more than \$Y within Z hours. (X, Y and Z are definable parameters at subscription to the alert)

In both cases report only once when it crosses the threshold, and the next report should be when the threshold is regained and then crossed again



Solution Requirements

- Functional :
 - Capability of receiving information in various types and format
 - Apply different event correlation patterns and conditions:
 - **Aggregation** of values reported by several messages > X
 - **Counting** of messages > X
 - ...
 - Semantic context awareness in order to correlate messages based on account number
 - Temporal context awareness (a floating time window of Z hours)

- Non Functional
 - Various types of message formats
 - Constantly changing customer requirements
 - Support delayed message processing for out of order message arrival
 - Flexibility (new types of alerts, new sources of input, new actions)
 - High availability
 - High throughput
 - Recovery

The Solution – Use WebSphere Message Broker with CEP Nodes

Provide *timely* and effective notifications through sending service data through Customer Alert system

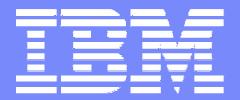


Integrate and mediate disparate systems, programming languages from advanced ESB features in WebSphere Message Broker



"With the complex event processing capability of WebSphere Message Broker we can better manage business risk, for us and our customers, by automatically identifying and responding to complex series of events that signal possible breaches of our thresholds before they actually occur. – Bank IT Manager

Apply Complex Event Processing to detect complex rules over message history to provide useful and effective alerts



Event-based Middleware & Solutions group

CEP in Products and Solutions



CEP in IBM and Business Partners products and solutions

- Products

- Websphere Message Broker CEP Detector Nodes
- WBI Server Express business rules
- CEP is embedded in IBM's business partner, Bristol Technology, product
- CEP is embedded in IBM's business partner, Syncron, product

- Solutions

- Trade Processing - Transaction Monitoring and Exception Management (financial markets)
- CEP for Underwriting GBS asset (insurance)
- Insurance Service Hub GBS asset (Insurance)



WBI Message Broker CEP Detector Nodes

- Two CEP based Websphere Message Broker processing nodes:
 - **SituationManager** node – performs an observation task
 - **IntelligentFilter** node – performs rule based routing
- The CEP Nodes provide functionality beyond the traditional Message-At-A-Time processing model.
- Runtime definition update – no need to restart the system

Link to WMB CEP Detector Nodes

<http://www-306.ibm.com/software/integration/support/supportpacs/category.html#cat3>



CEP for Underwriting - Insurance Solution (An IPSC asset)

Enable event driven rules in insurance underwriting process

Challenge

- Automate business processes, based on rules, to enable Straight Through Processing for consistent and faster underwriting decisions
- Add new intelligence to business processes—without the need for full transformation of legacy systems or intensive code development
- Reduce development cycle by providing top down model based methodology
- Incorporate state-of-the-art rules, methodology, and technology

Solution

- This solution establishes a framework for underwriting in insurance engagement, using business rules and complex event processing (CEP) capabilities
- Complex Event Processing for underwriting leverages CEP technology, by populating it with insurance content (business rules) and defining best practices for using CEP concepts in insurance engagements
- The result is a reusable and executable set of business and CEP rules that maximize business agility.

Benefits

- Underwriting processes become faster, more agile and consistent
- Faster time to market by jumpstarting the project with the pre-populated rules
- Lower project risk, by leveraging best practices and code already sold in the market
- Lower total cost of ownership, by substituting labor costs with the cost of the licensed asset



Insurance Service Hub - Auto Claims (An IPSC asset)

Claim Processing Hub

- Connecting insurance carriers, auto body shops and appraisers

Challenge ▪ The IBM Insurance Service Hub supports the exchange and validation of business information throughout the claims management process

Solution ▪ The hub focuses on the area of car claims and supports the exchange of business information between insurance carriers, body shops and appraisers. It is not a claims application substitute but rather, complements core insurance functionality

▪ The hub enables receiving data about a car claim from different information sources, structuring relevant claims data into a common XML-based format and validating the data by applying complex business rules and a leading automotive industry data base against the claims documents

Benefits ▪ Systematic identification of savings potential in claims documents

▪ CEP business rules identify approximately > 10% savings potential in appraisals on the average

▪ Efficient use of appraiser organisation

▪ Reduction of car rental cost due to reduce process cycle time

▪ Reduction of payments for loss of use in liability



RFID Integrated Tracking & Alerting System

Challenge

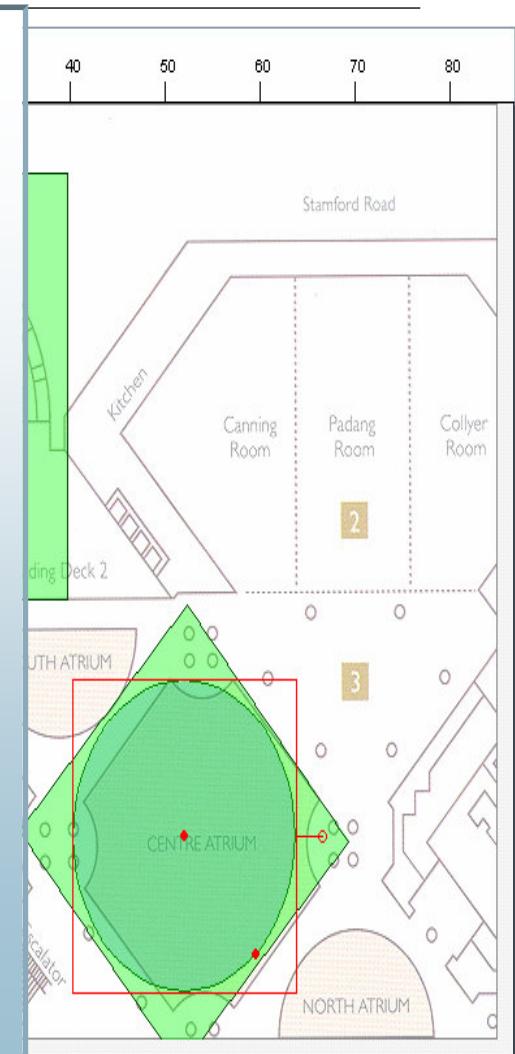
- Work units are not correctly synchronized between kitting and building operations
- Locating work units on the factory floor is adding unnecessary time to the build cycle

Solution

- An intelligent and customizable item tracking system featuring:
 - Using Active RFID zonal tracking.
 - Deployment modeling Tool which Supports floors mappings, zones setup and Intuitive graphical feedback.
 - Complex Event Processing – used to generate alerts and reports according to predefined rules, related to the items location reports. While considering the reports time, For example: alerting when item arrival to an area extends the expected time.

Benefits

- Reduced cycle time
 - More productivity
 - Increased manufacturing capacity
 - Reduced inventory carrying costs
- Less chance of handling damage
- Increased accountability through reporting
- Extend application to other areas of supply chain





Spatio-Temporal Event Detection Service

Challenge

- Enabling detection of vehicle's internal condition as well as the vehicle's relationship with fixed and mobile entities.
- Enabling detection of driver's physical condition and alerting abnormal situations.

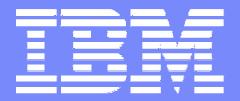
Solution

- The service is designed to simplify the development of applications by providing a high-level rule-based programming environment.
- Programmers represent events of interest in the form of rules that "trigger" when the situations are detected.
- Rules operate on both input received from the data acquisition systems as well as data resources provided and managed by the application programmers.

Benefits

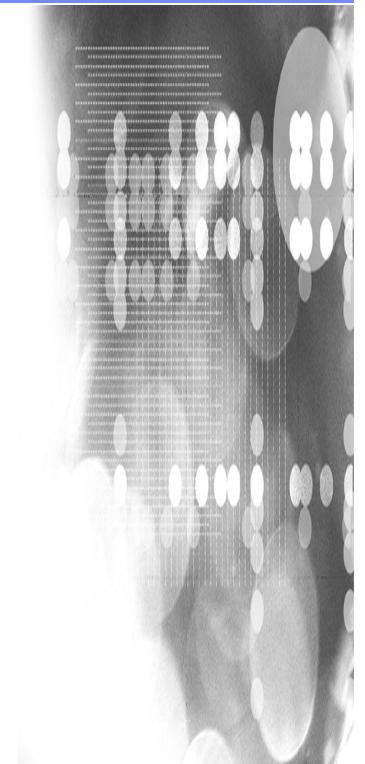
- STEDE serves ubiquitous-computing applications that involve sensing conditions in a user's physical context and responding to those conditions in real time.
- Alert drivers when they are off-route or off-schedule
- notify fleet operator that truck is entering the loading zone
- location-based promotions services that notify consumers of special sales in a nearby store.





Event-based Middleware & Solutions group

Customer References



Retail Bank

Superior Customer Service with SOA Exploitation of CEP technology

Challenge

- Need for Customer Alert System to send alerts on account and credit status, daily notifications and stock prices.
- IBM had to enable the receipt of data from multiple sources, types and format, and apply Complex Event Processing to detect complex rules over message history to provide useful and effective alerts.
- Need to transform, route, and apply various data for an integrated customer alert system

Solution

- In this case the focus was on Aggregation (e.g. report if the withdrawals from an account exceed a certain number of USD within a certain number of days) and Threshold (e.g. report when account balance crosses a threshold).

Benefits

- Provide timely and effective notifications to clients through customer alerting system providing differentiator from competitors
- Apply Complex Event Processing to detect complex rules over message history to provide useful and effective alerts
- Support for SOA



Bank

CEP for monitoring FIX gateway

Challenge

- The Bank finished acquisitions of 3 private banks. The bank is in the midst of technical and operational integration.
- Add in the business challenge of the integration of multiple banks
- Aware of status\problems with BJB financial brokering system - on time (customer satisfaction, cost reduction in problem solving)
- Aware of status\problems with brokers - on time (same as above including broker SLA enforcement)

Solution

- FIX Broker Session Monitoring (such as a connection to a partner's FIX broker is lost)
- FIX Broker Message Monitoring (such as FIX Broker validated, committed and sent a particular FIX message within a predefined time – an acknowledged situation)
- FIX Message (such as an execution report (of either success or failure) has not been received within a predefined time for a customer for which a new order was sent or detect that a situation above occurred and later an execution report was received for that particular order.)

Benefits

- Systematic identification of savings potential in claims documents
- CEP business rules identify approximately > 10% savings potential in appraisals on the average
- Efficient use of appraiser organisation
- Reduction of car rental cost due to reduce process cycle time
- Reduction of payments for loss of use in liability



Continuous Audit

CEP for risk & compliance

Challenge

- Need to extract information from existing systems to monitor real time high risk transaction exceptions based on predefined criteria.
- Internal audits in enterprise are struggling with the challenge to be able to monitor the information exchange within the enterprise and to external customers and suppliers

Solution

- Prompt identification of potential high risk control exposures
 - Supplements the organization's internal control framework
 - Augments monitoring of KCFR
 - Proactively complements the organization's testing
- Reduce potential for revenue overstatement through prompt identification of process bypasses
- Provide management with the opportunity to immediately correct potential anomalies as they occur
- Improve productivity and efficiency of auditors (Reduce audit travel and face to face time with line management)
- Real-time oversight will help to reduce undesirable behavior

Benefits

- Accesses predefined data elements from multiple applications
 - Provides vehicle for linking potential risks (e.g.. large order placed at quarter end with A/R delinquencies)
 - Allows flexibility to modify selection criteria for potential control exposures
 - Has capability to notify designated individual (s) on a daily basis of potential control exposures to assess



Healthcare

Using RFID to Track Emergency Room Patients at the University Hospital of Nice

- Optimization of the patient path in the Hospital's Emergency Unit in terms of:

Challenge

- Patient traceability
- Eliminate patient friction
- Reduce delay or unnecessary waiting times

Solution

- Optimization was done through the use of RFID Wireless technologies and CEP
- CEP is used to optimize patient path in Emergency Unit. For instance, when a patient arrives to the emergency Unit, he is registered (this event is sent to the CEP engine) and then directed to the Medicine area to meet a physician. When he enters this area this localization event is also sent to the CEP engine and a time frame is initialized. If the patient isn't seen by the physician after this predefined time frame, an alert is sent to the system notifying that this patient have been waiting for a too long period.
- http://w3.ibm.com/news/w3news/top_stories/2005/11/europe_nice_hospital.html

Benefits

- Customer satisfaction (better and faster service for patients)
- Optimized process
- Traceability and Statistical analysis are possible





Pharmaceutical

CEP for Contract and Sales Validation

Challenge

- Need to support automatic contract validation against actual sales
- Contract validation is manual and as a result inconsistent, error pruning and time consuming
- Need to support context capability (both semantic and temporal)

Solution

- CEP was used as a rule system that has a temporal context and can be used easily to write numerous rules that are very similar (using a predefined set of templates)
- The rules serve to verify that the actual sales data entered by the sales people fit the contracts that were signed with clients.

Benefits

- CEP enables Roche to validate contracts signed with its customers, and compare actual sales with the contract
- Reduce time and costs
- Consistent decisions

