



OBJECT MANAGEMENT GROUP

## Workshop on Distributed Object Computing for Real-time and Embedded Systems

July 14 – 16, 2008, Washington, DC, USA

 **TIBCO**<sup>®</sup>  
The Power of Now<sup>®</sup>

**Paul Vincent**  
*TIBCO Software Inc.*

# Complex Event Processing Tutorial



- **Presenter:**  
**Paul Vincent, CTO Business Rules and CEP, TIBCO Software**
  - Member OMG PRR and W3C RIF rules standards bodies
  - Co-author CEP Blog <http://tibcoblogs.com/cep>
  
- **TIBCO Software Inc.:**
  - Provides enterprise software that helps companies achieve service-oriented architecture (SOA) and business process management (BPM) success
  - Headquartered in Palo Alto, California
  - Over 3,000 customers and offices in 40 countries
  - CEP product is TIBCO BusinessEvents
    - Developed from a customer solution and launched 2005
    - Currently at Release 3.0

## ■ Introducing CEP

# Real-world Events

Customer Logon

Fed Base Rate Increase

Customer Checks  
"Close Account"  
Web Page

New Order

Production Item Arrives at Store

New Liability Added

Mobile Call from CT @11.13

Contract Submitted

Rental Car Crashed

Rental Car Returned

Contract Returned thru EDI

**Customer  
Logon**

**Fed  
Base Rate  
Increase**

**Customer  
Checks  
Close Account  
Web Page**

**New  
Order**

**Production  
Item  
Arrives at  
Store**

**New  
Liability  
Added**

**Mobile Call  
from CT  
@11.13**

**Contract  
Submitted**

**Rental  
Car  
Crashed**

**Rental  
Car  
Returned**

**Contract  
Returned  
thru EDI**

**Fraud  
Risk!**

**Risk of  
Customer  
Defection**

**Customer  
CrossSell  
Opportunity**

**Change in  
Product Sales  
Trend**

**Employee  
Over hours**

**Compliance  
Limit  
Approached**

**Cell phone  
fraud alert**

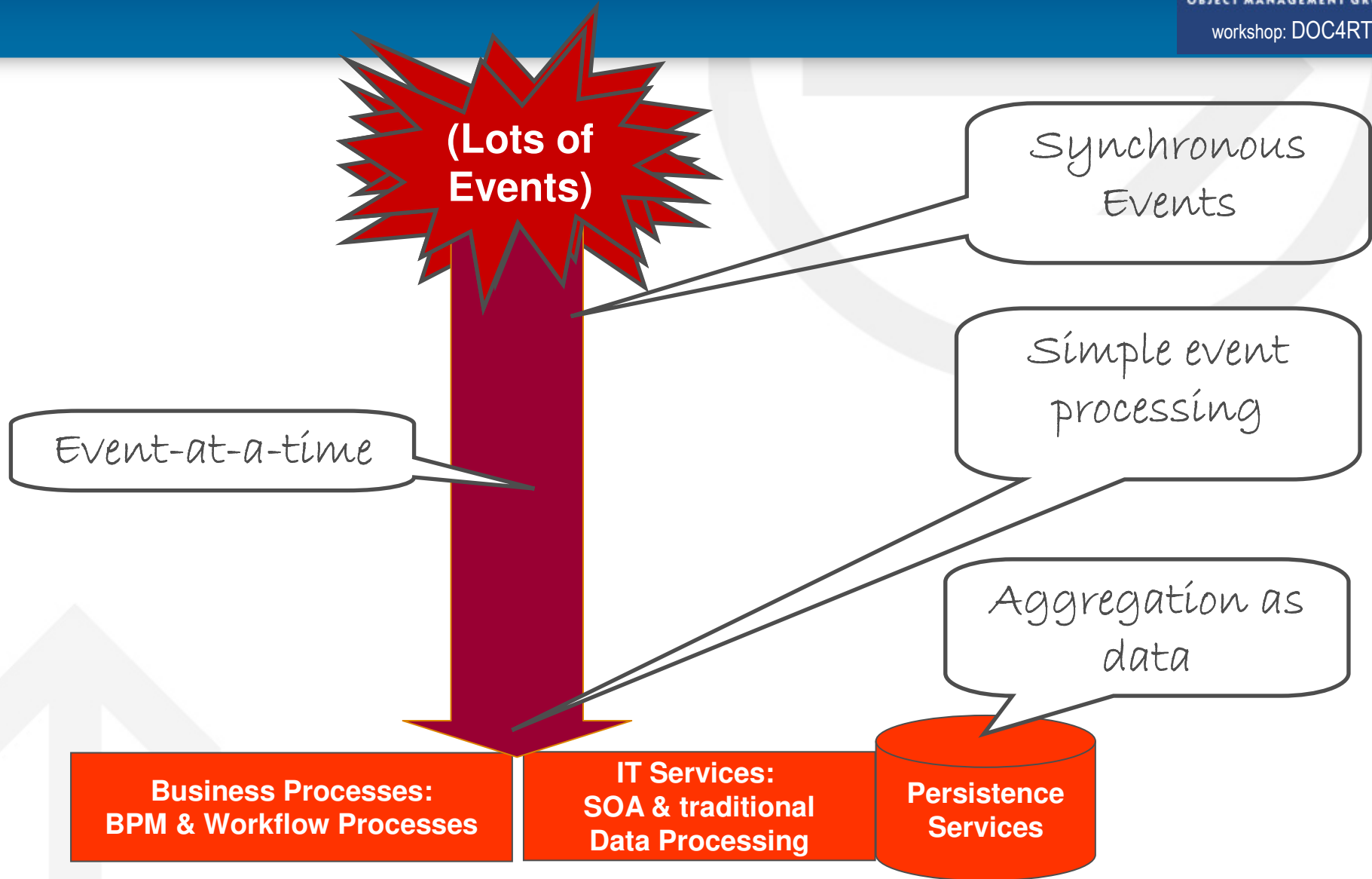
**Contract  
Validated**

**Rental  
Contract  
Complete**

**Customer  
now rated  
Gold**

**Contract  
Valid**

# Conventional Event Processing



# Simple EP = default IT Model, 1950-now

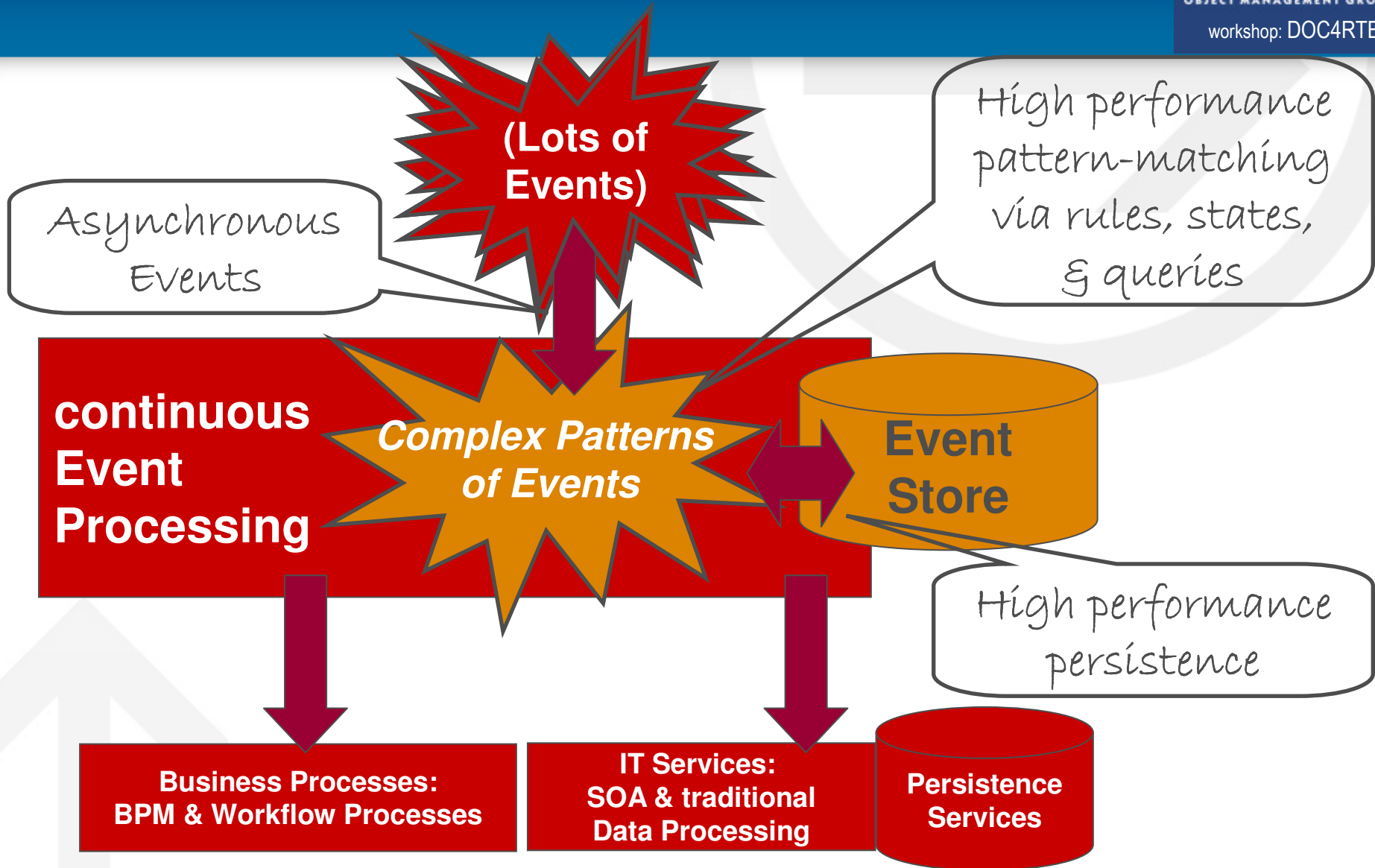
- **Based on “human workflow”**: one thing at a time
  - Processes handle cases 1 at a time ← office clerk
  - Use database and refer to it where necessary ← card index
  - Provide some service flexibility with middleware ← internal mail
  - Use BPM to document / manage / automate processes
  - Use SOA to distribute / manage / automate services

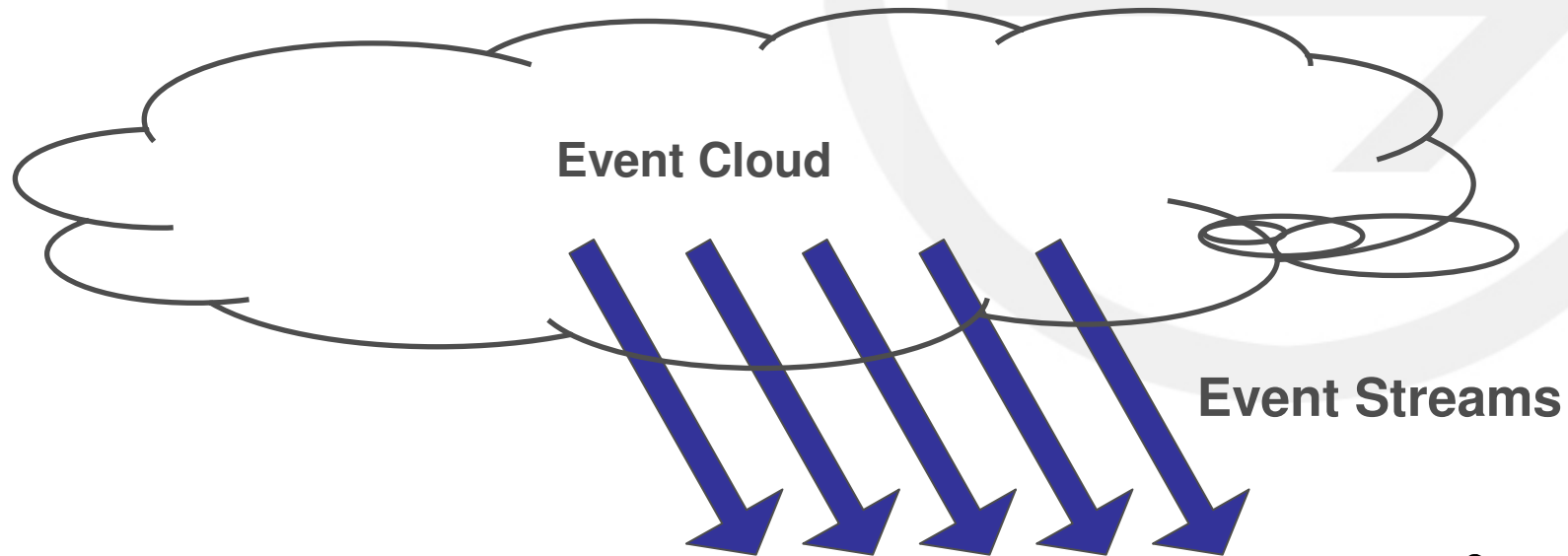
**This model does NOT exploit  
ALL the information / data / events  
ALL the time**

**Behaviour (and business logic) is silo'd**

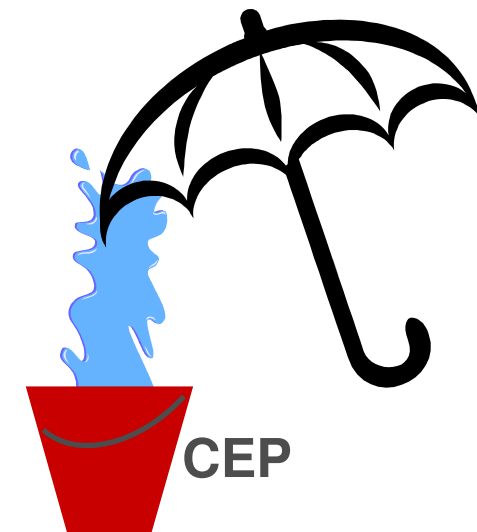
**There is a better way!**

# Complex Event Processing





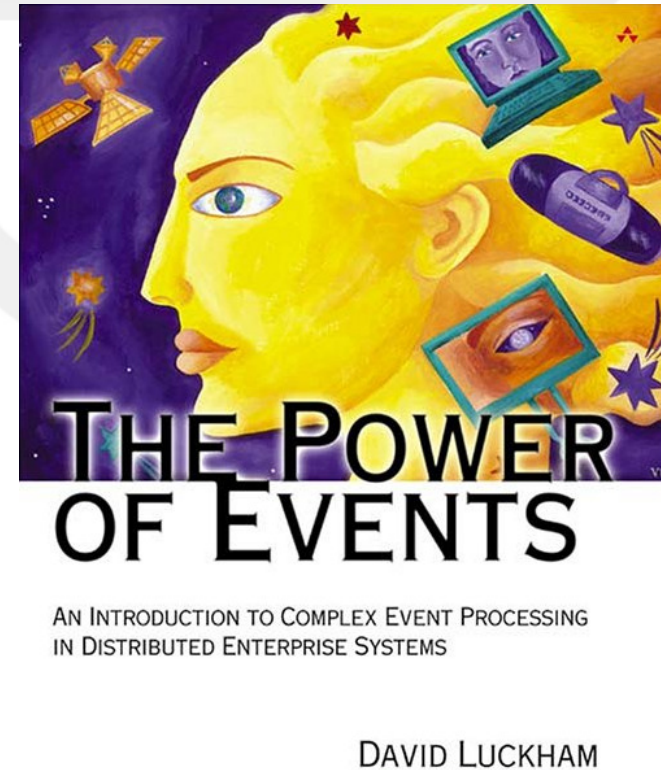
- CEP (technology) applies pattern detection & filtering to the event clouds & streams and their histories
- Multiple modelling / execution paradigms are available for pattern detection



# What does CEP cover?

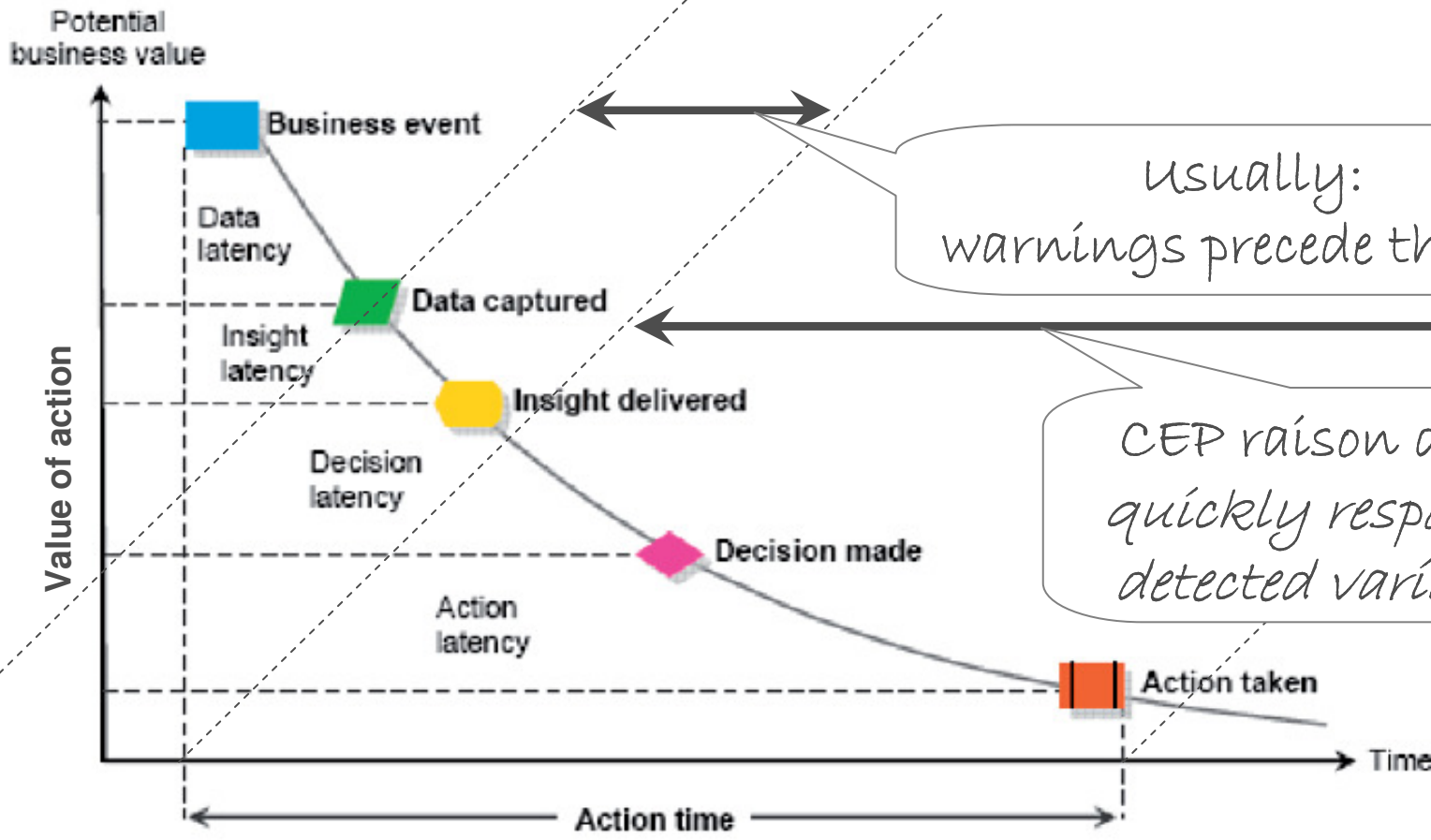
***“CEP applies to a very broad spectrum of challenges in information systems. A short list includes:”***

- Business process automation
- Computer systems to automate scheduling and control network-based processes and processing
- Identifying when complex contracts are fulfilled
- Detection intrusion, fraud and other network attacks
- C3I



**The Power of Events, Addison Wesley, ISBN: 0-201-72789-7, 2002**

# What does CEP Solve?



**Figure 1:** The steps involved in taking action to respond to business events

the "Latency Problem"

**“Situational Awareness”**

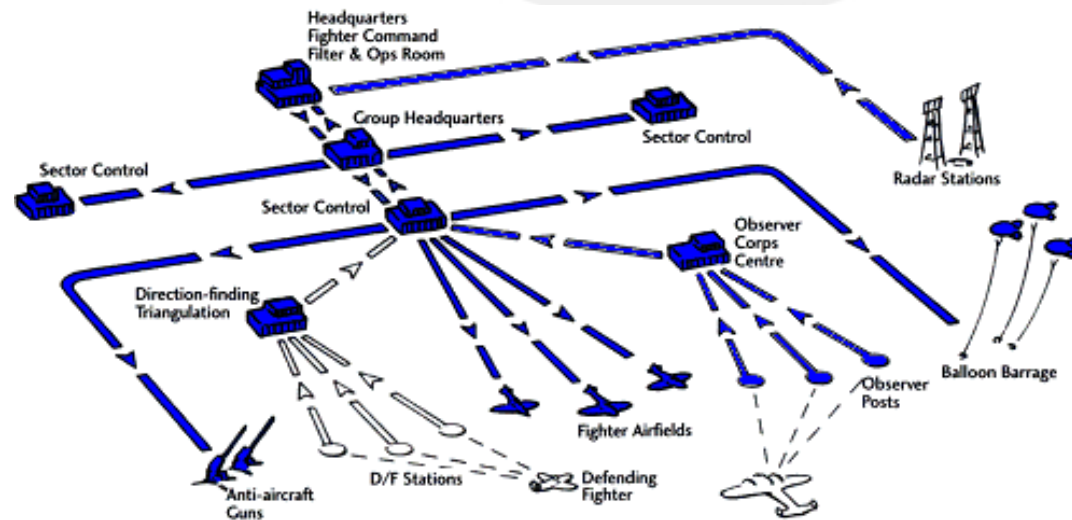
**“Sense and Respond”**

**“Track and Trace”**

## ■ History

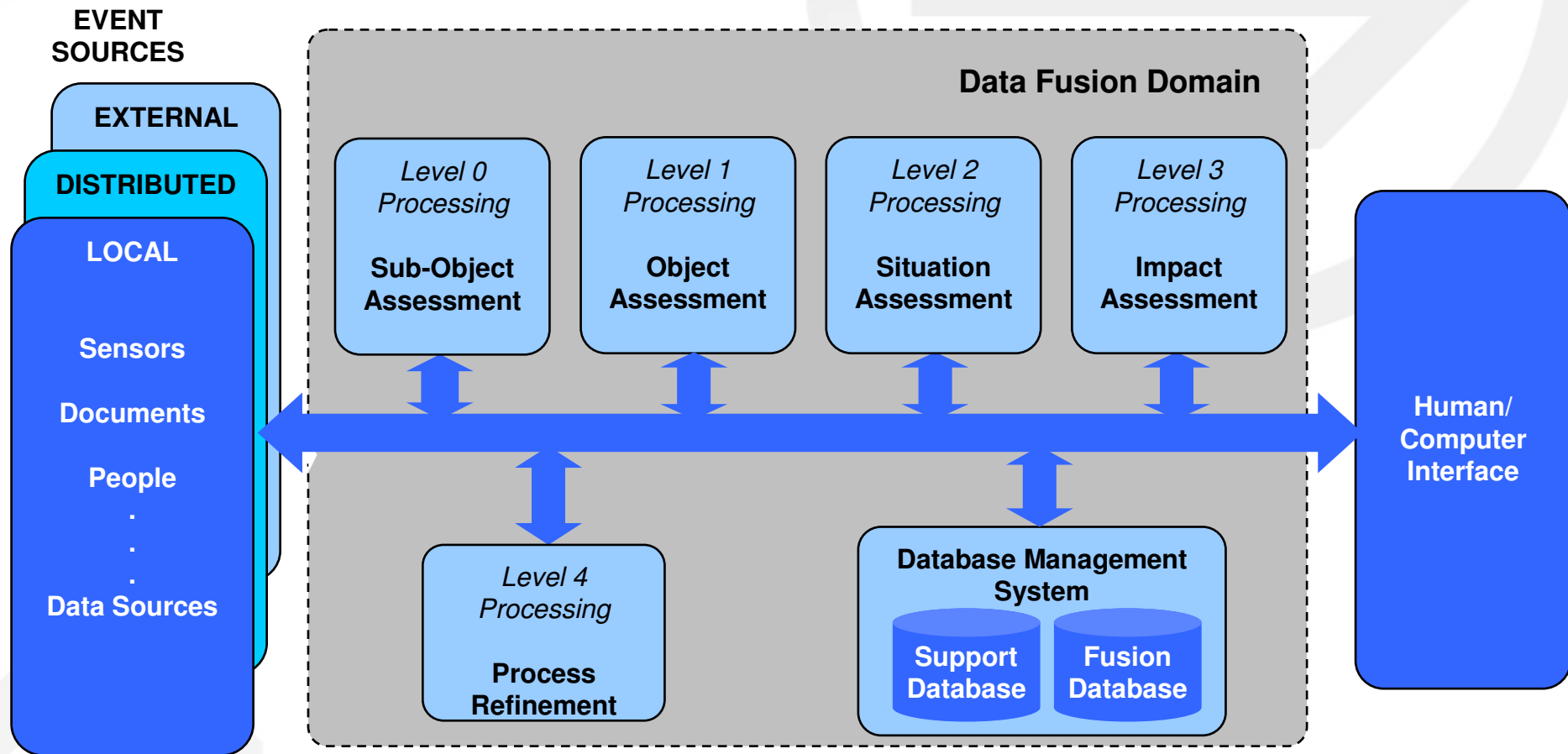
- **Command and Control**

- Correlate all available information
- Determine tactics based on strategy and up-to-date information



-- from RAF Battle of Britain Fighter Control System 1940  
<http://www.raf.mod.uk>

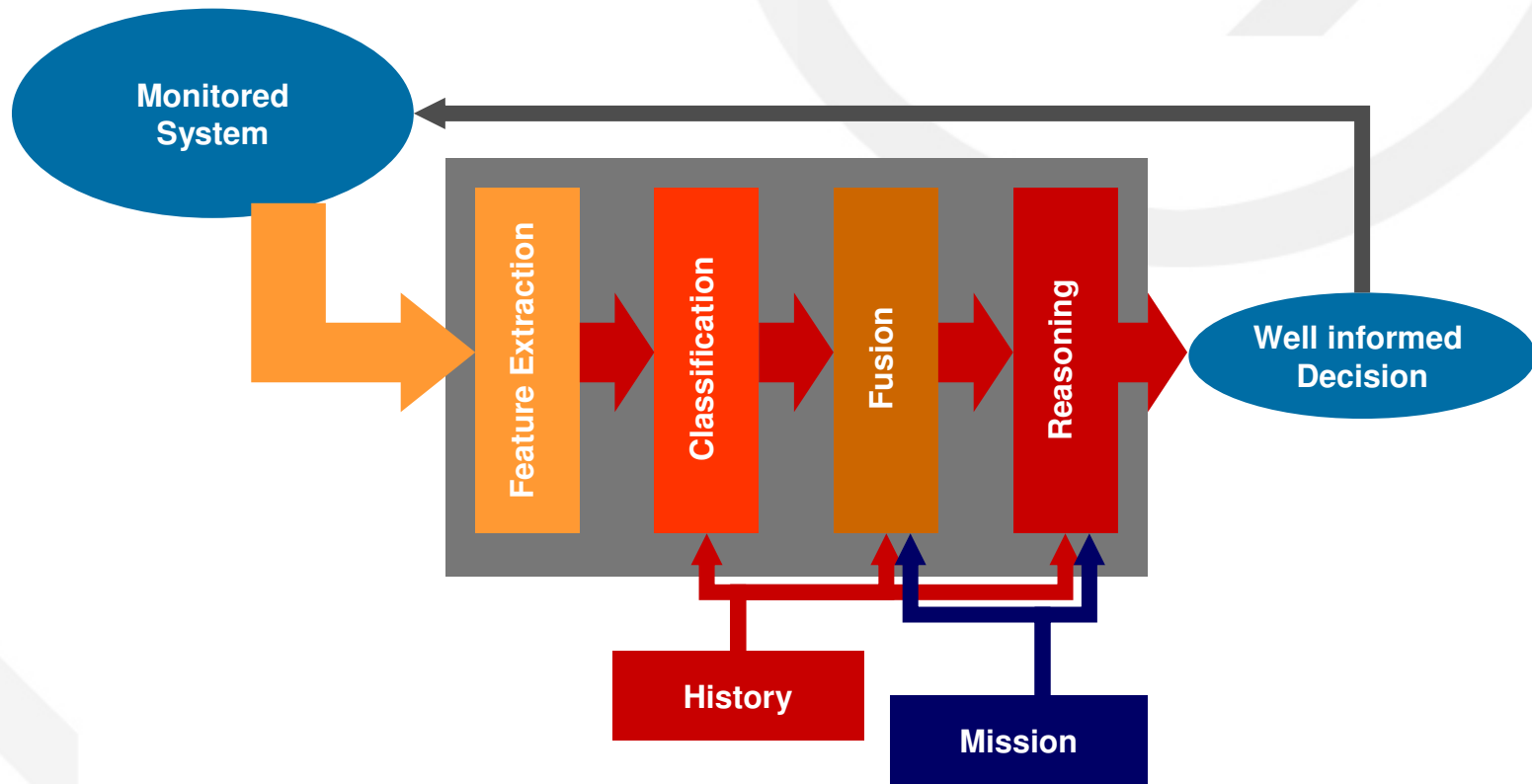
# Data Fusion



-- Revised JDL data fusion model, 1998

Steinberg, A., & Bowman, C., Handbook of Multisensor Data Fusion, CRC Press, 2001

# Condition Based Maintenance



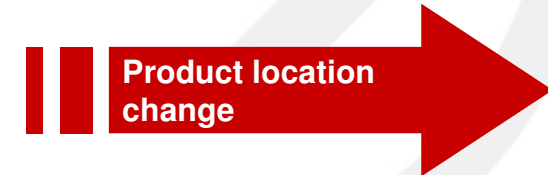
-- from "Data Fusion for Developing Predictive Diagnostics for Electromechanical Systems"  
Steinberg, A., & Bowman, C., Handbook of Multisensor Data Fusion, CRC Press, 2001

## ■ Events and CEP

## ■ Fraud / Theft

- Thousands-to-millions of high-value small-size product items or transactions
- How do you identify known patterns of “suspicious” behavior?

Relevant event of interest



## ■ Logistics / Scheduling

- Raw material, production & delivery scheduling and resources are complex and prone to change
- How do we reallocate resources to handle business and production changes?



## ■ Activity Monitoring

- Complex production and supply process with multiple actors
- How to measure and action Key Performance Indicators?



# Associated Events

## ■ Positive Events

- Product item X arrives at Production station S from Store T
- Production worker Y arrives at Production station S
- Production contract for item Z by time T is posted



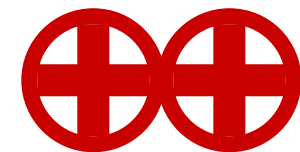
## ■ Negative Events

- Product item X has been in transit to Store T for >15 minutes
- Subcomponent Y hasn't arrived at the Production station by the ETA
- Delivery of contract Z has not taken place



## ■ Sets of Events

- 5+ items of Product item type Y failed to arrive at destination
- Supplier Y was 5 mins late for 1 delivery, but made it early to the next
- Return rate on component Z exceeds SLA %



# Significant features of these Events

## ■ Time Sensitivity

- A thief may leave the building at the same time as stolen product
- A product should take 40 minutes to travel a given production line segment



## ■ Distributed Event Sources

- A series of produced items fails at various QA stages, and their common attribute was a storage location
- Multiple suppliers for a subcomponent are reporting delivery delays



# What \*is\* an “event”?

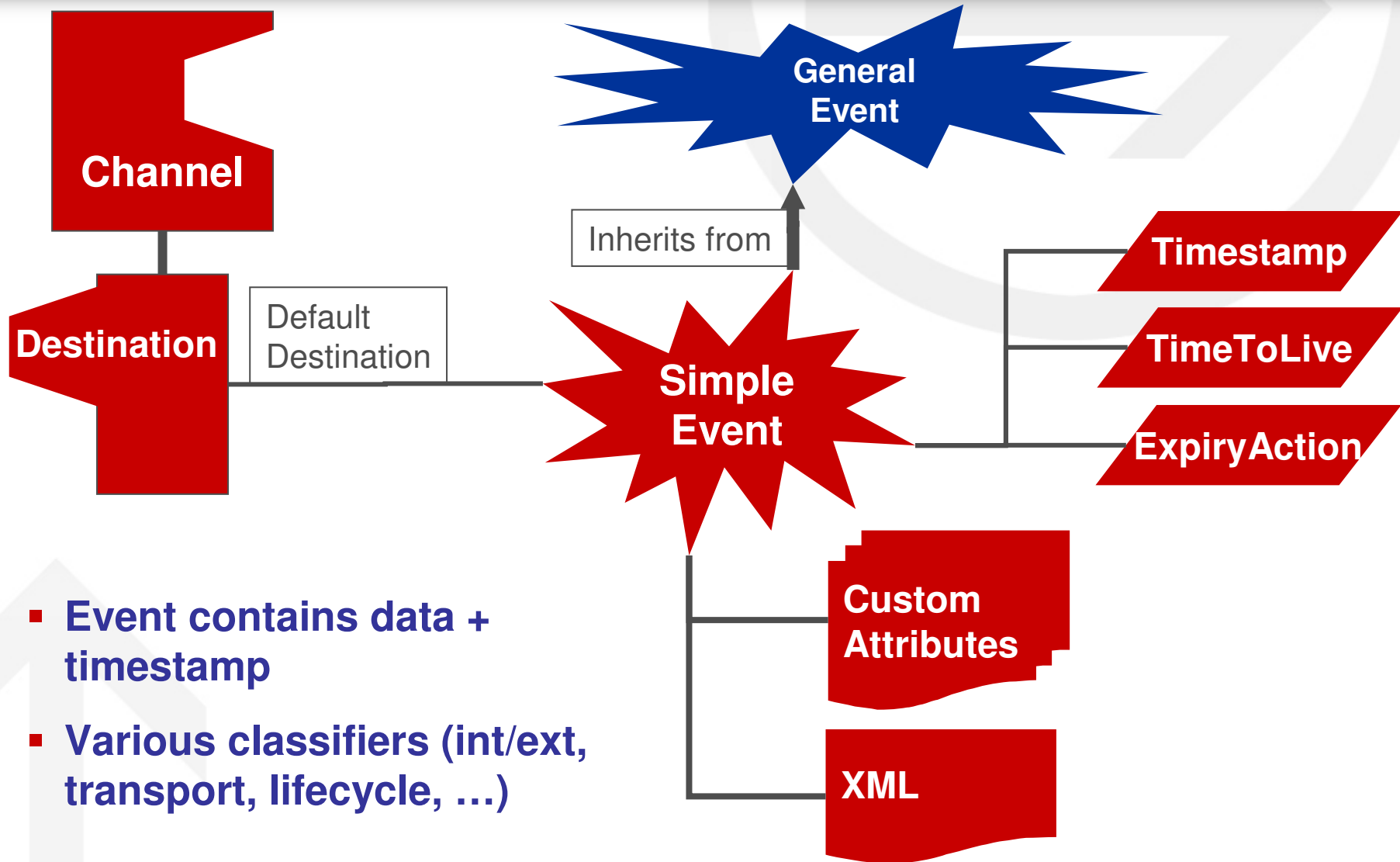
- **Change of state in some entity**
  - Customer call
  - Bank debit
  - Aircraft movement
- **Observation of some entity**
  - CRM record of a customer call
  - ATM report of debit transaction success
  - Radar plot update of an aircraft
- **IT Message**
  - Queued point-to-point message
  - Publish / subscribe message

“Happening”

Observation

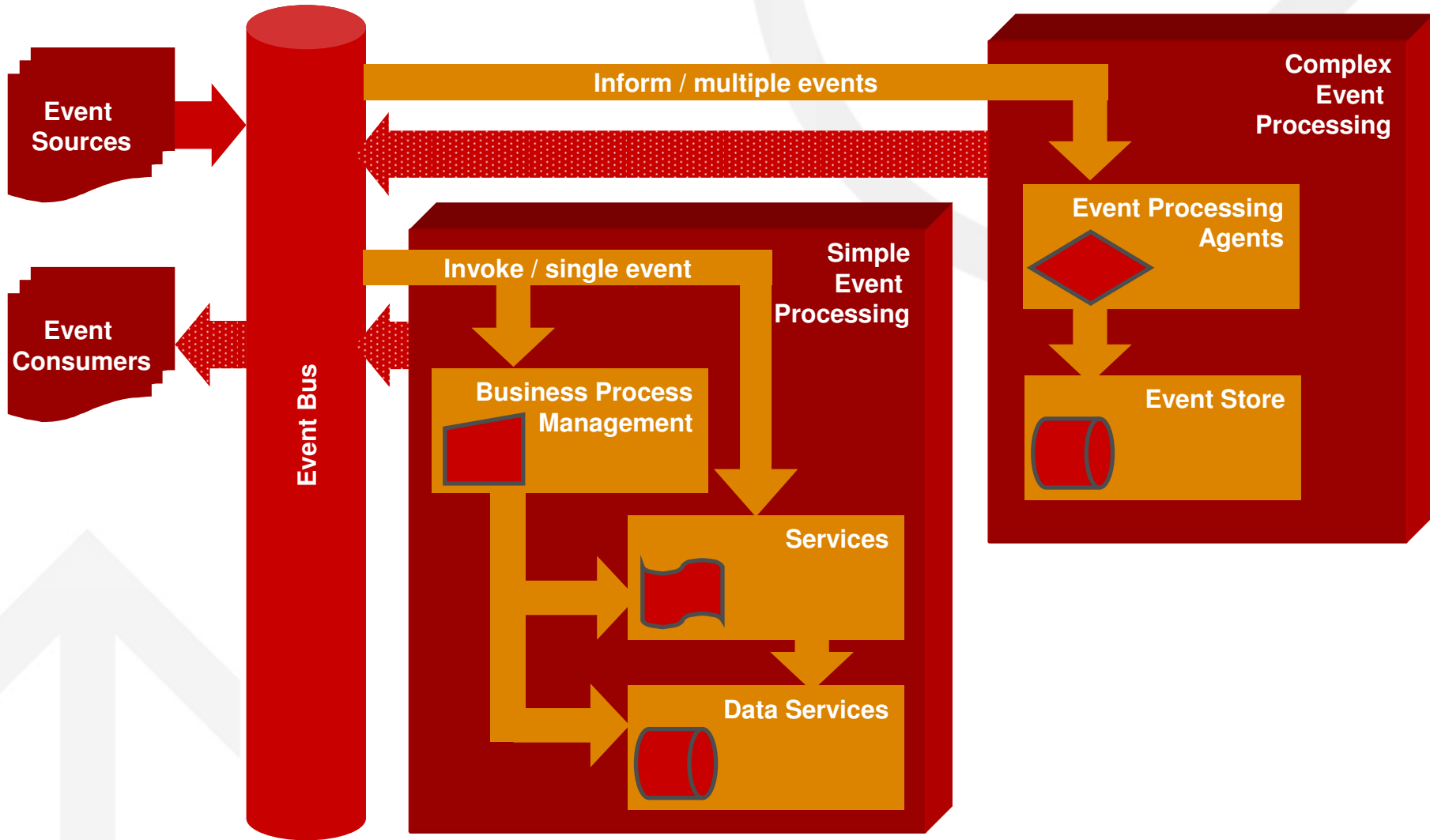
IT Message

# Sample Event Metamodel

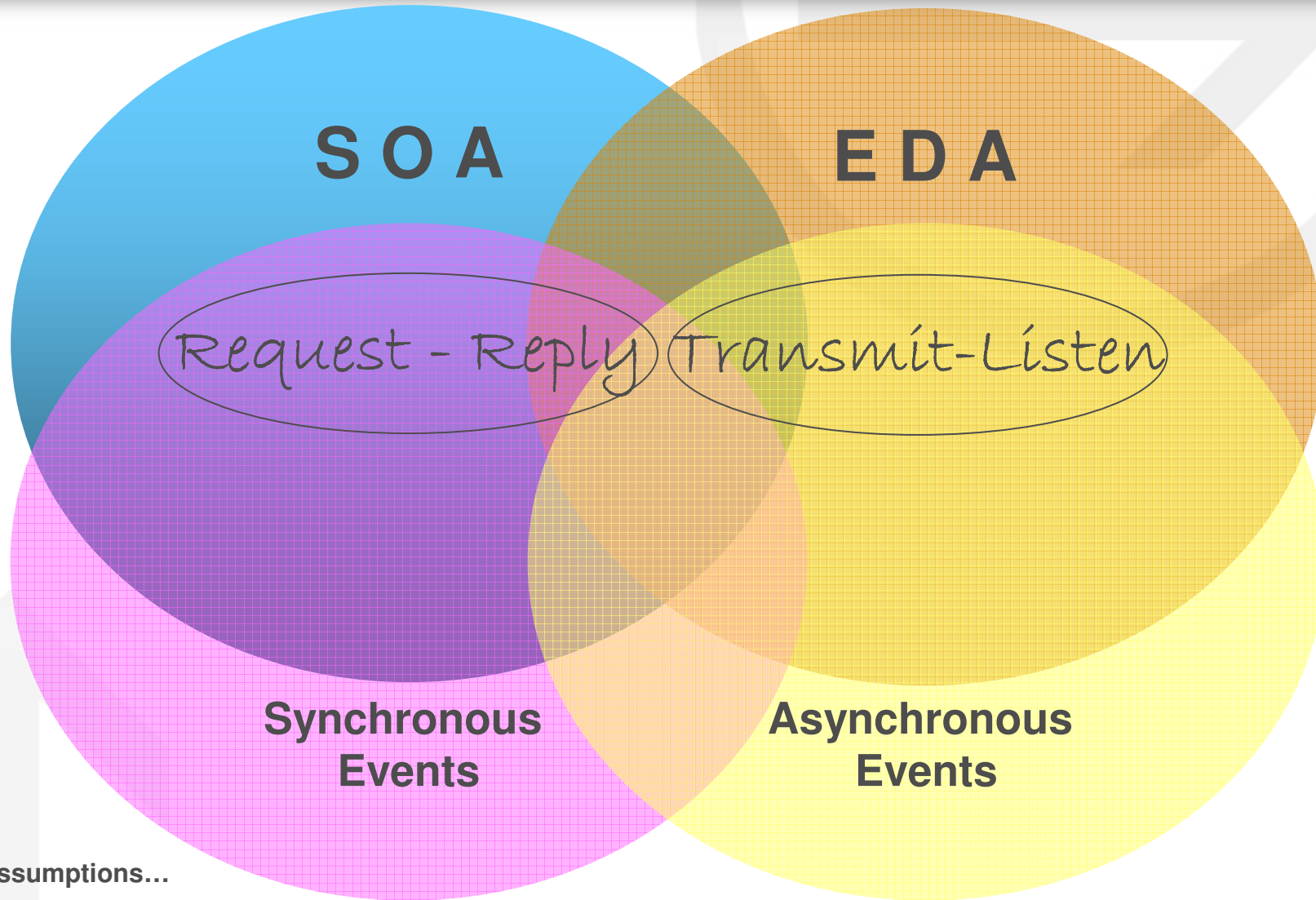


- Event contains data + timestamp
- Various classifiers (int/ext, transport, lifecycle, ...)

# Event-driven vs Event Processing

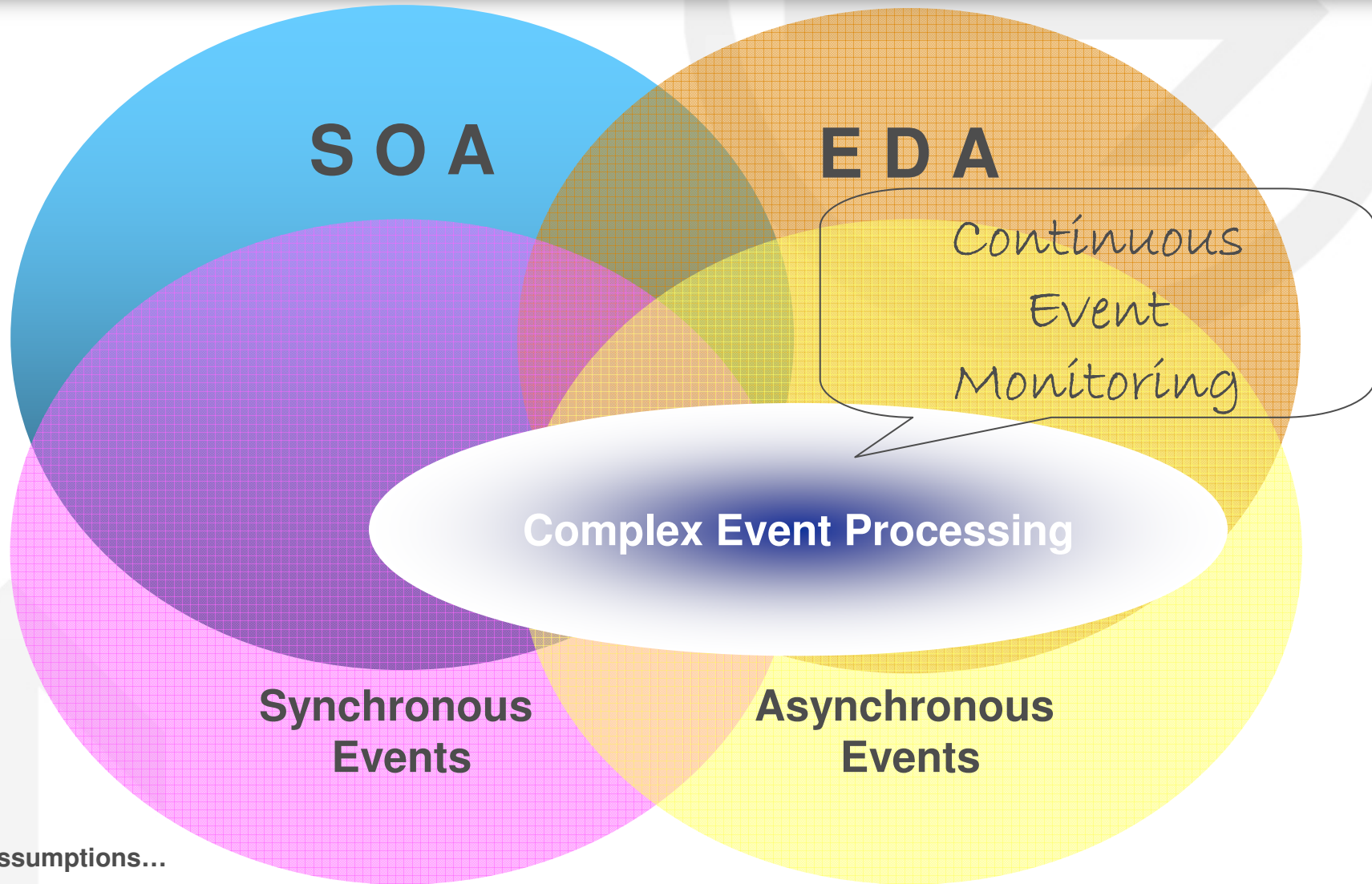


# Event Driven Architecture



Assumptions...

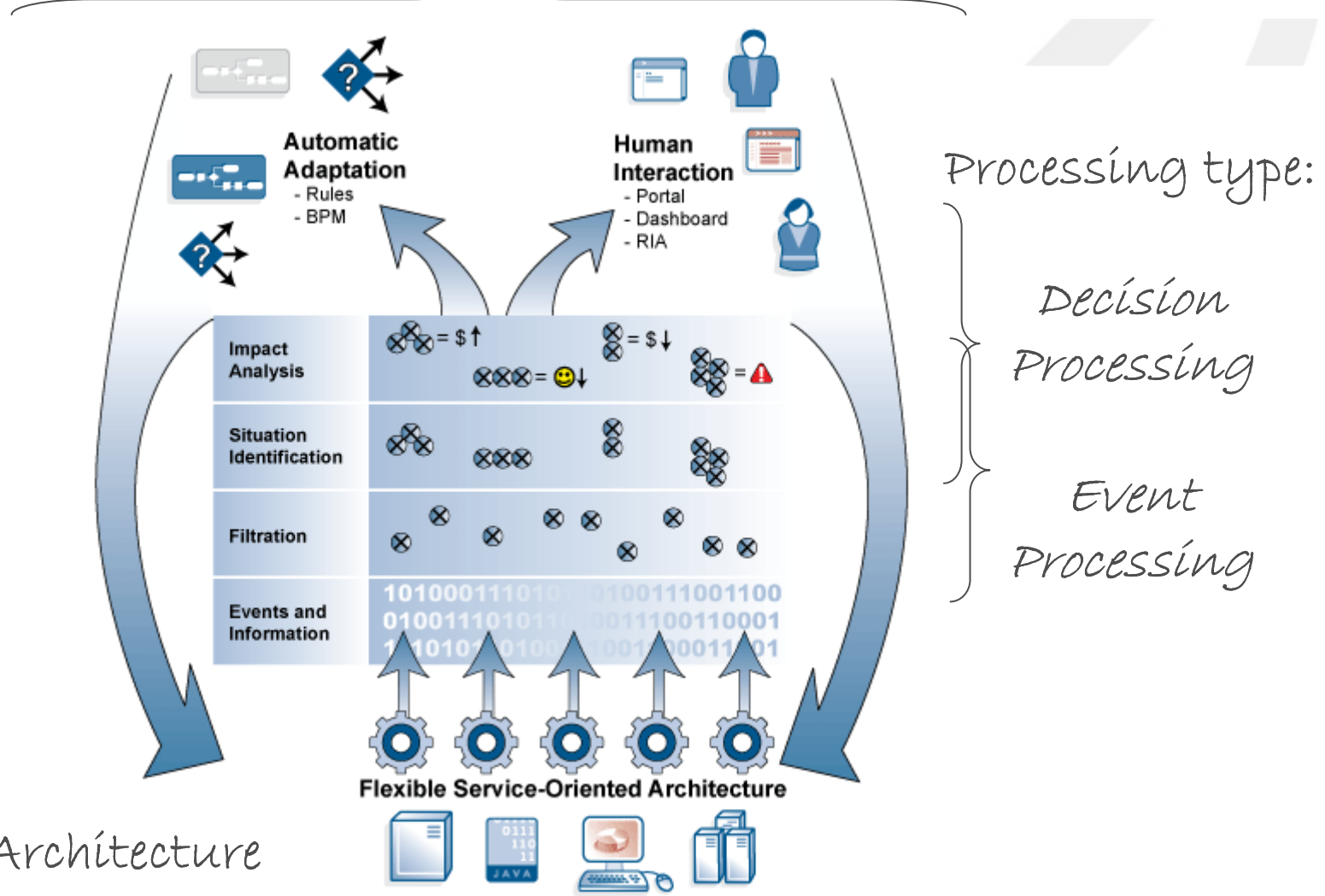
# CEP in the Event Driven Architecture



Assumptions...

# Complex Event Processing

*Sense and Respond / Track and Trace / Situational Awareness*



*TIBCO Reference Architecture*

Underlying Applications and Infrastructure

© 2008 TIBCO Software Inc. All Rights Reserved. Confidential and Proprietary.

# Analysts on CEP

Decision Latency →

**Gartner Summit Events**

**Gartner Event Processing Summit**  
Real Time Agility through Event Processing and Business Activity Monitoring

**19 - 21 September 2007**  
Orlando, FL  
JW Marriott Grande Lakes

- ▶ How to Contact Us
- ▶ Download PDF Brochure
- ▶ Request Event Information
- ▶ Build My Agenda

**Gartner.**  
Event Processing  
Summit 2008

## Gartner Event Processing Summit

15 - 16 September 2008 | Stamford, CT | Hilton Stamford Hotel

Event Complexity →

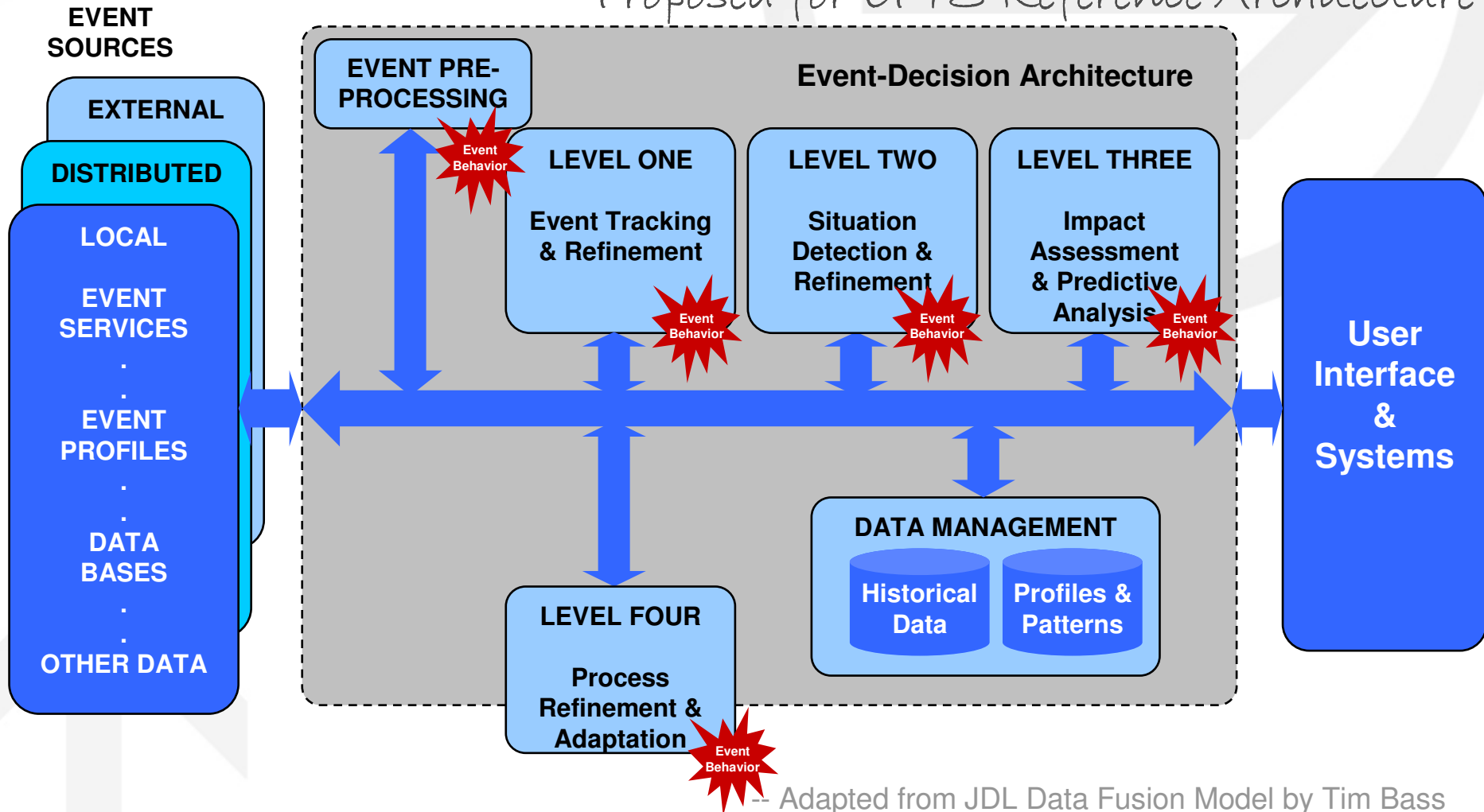
# Why CEP?

- **Detecting event patterns across multiple event types + time is difficult for simple event processing solutions**
- **Computers can correlate across large volumes of events at high speed, identifying patterns that are not conventionally visible**
- **The architecture pattern of “continuous event processing” applies to many business domains such as BAM**
- **Examples in use:**
  - **Track and Trace** of RFID data
  - **Situation Assessment** of airline operational delays (+ their causal events)
  - **Sense and Respond** to fraud indicators in internet transactions

## ■ CEP Technologies

# CEP = an Event-Decision Architecture

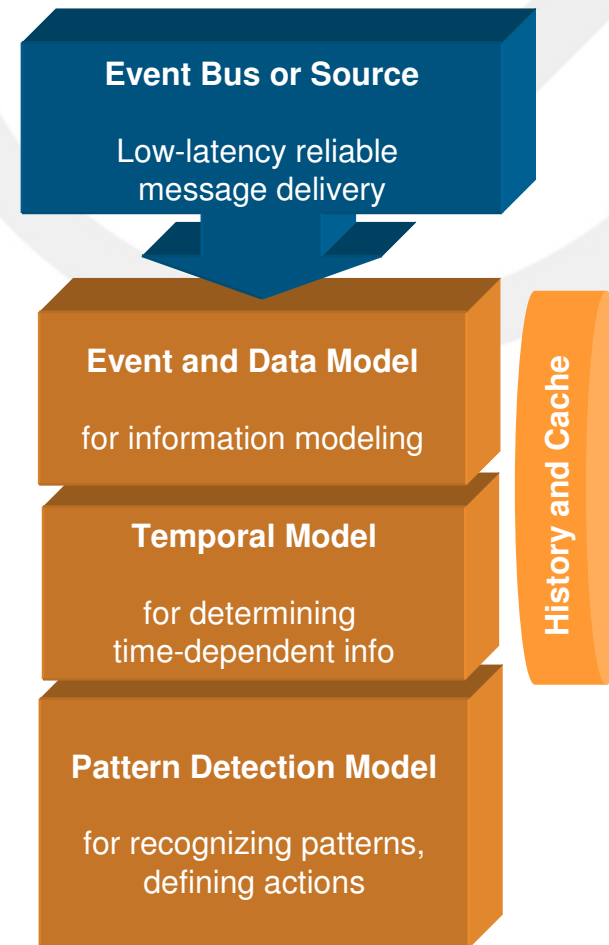
*Proposed for EPTS Reference Architecture*



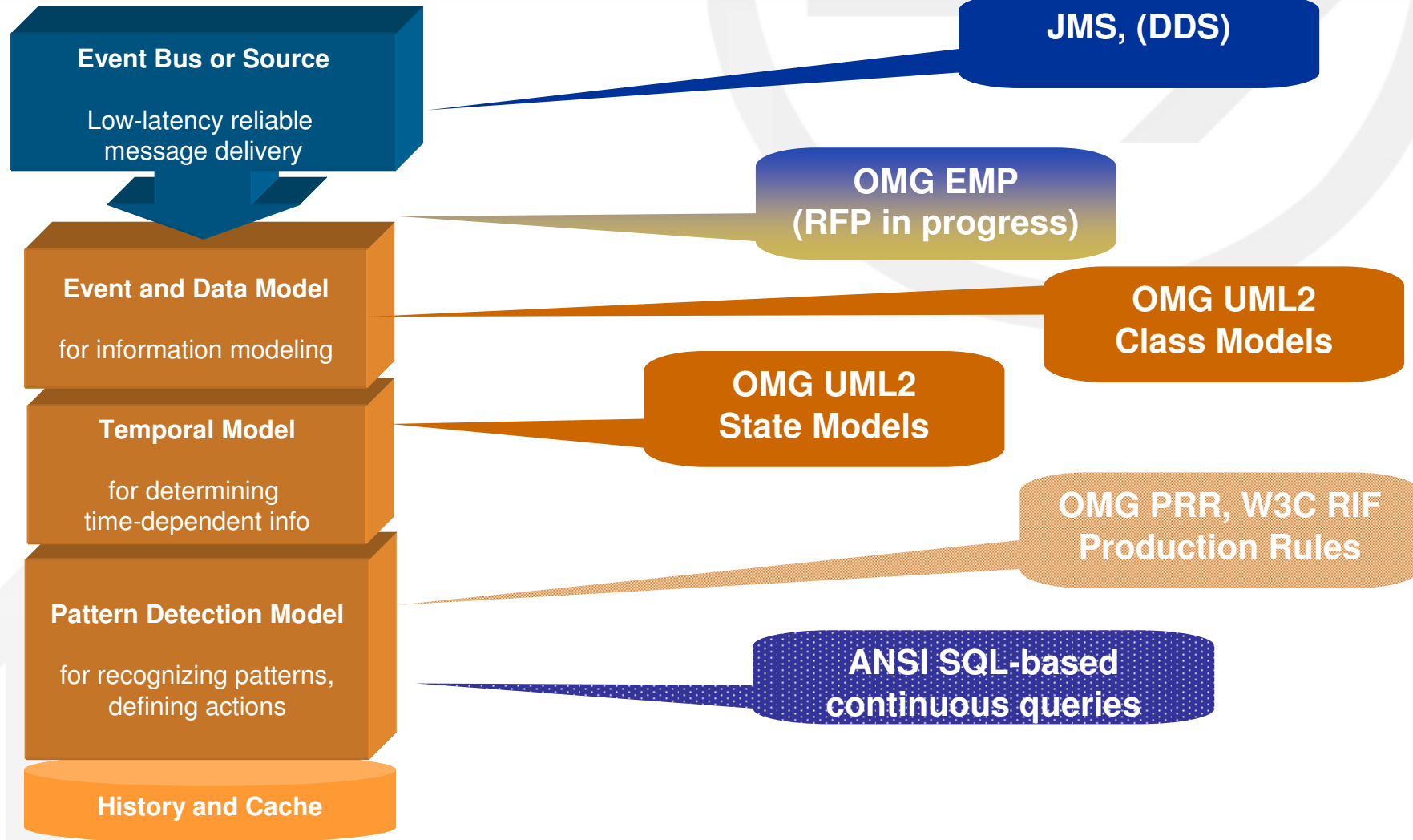
-- Adapted from JDL Data Fusion Model by Tim Bass  
Steinberg, A., & Bowman, C., Handbook of Multisensor Data Fusion, CRC Press, 2001

# Requirements for CEP Technology

- **Access and Monitor the “Event Cloud”**
  - JMS, RV, MQ, TCP/IP, etc...
  - Timers to detect lack of events
  - Determine event state changes
- **Match Patterns, Apply Business Logic**
  - Detect events
  - Detect event patterns
  - Maintain State and Facts over time
  - Update Detection algorithms as events change



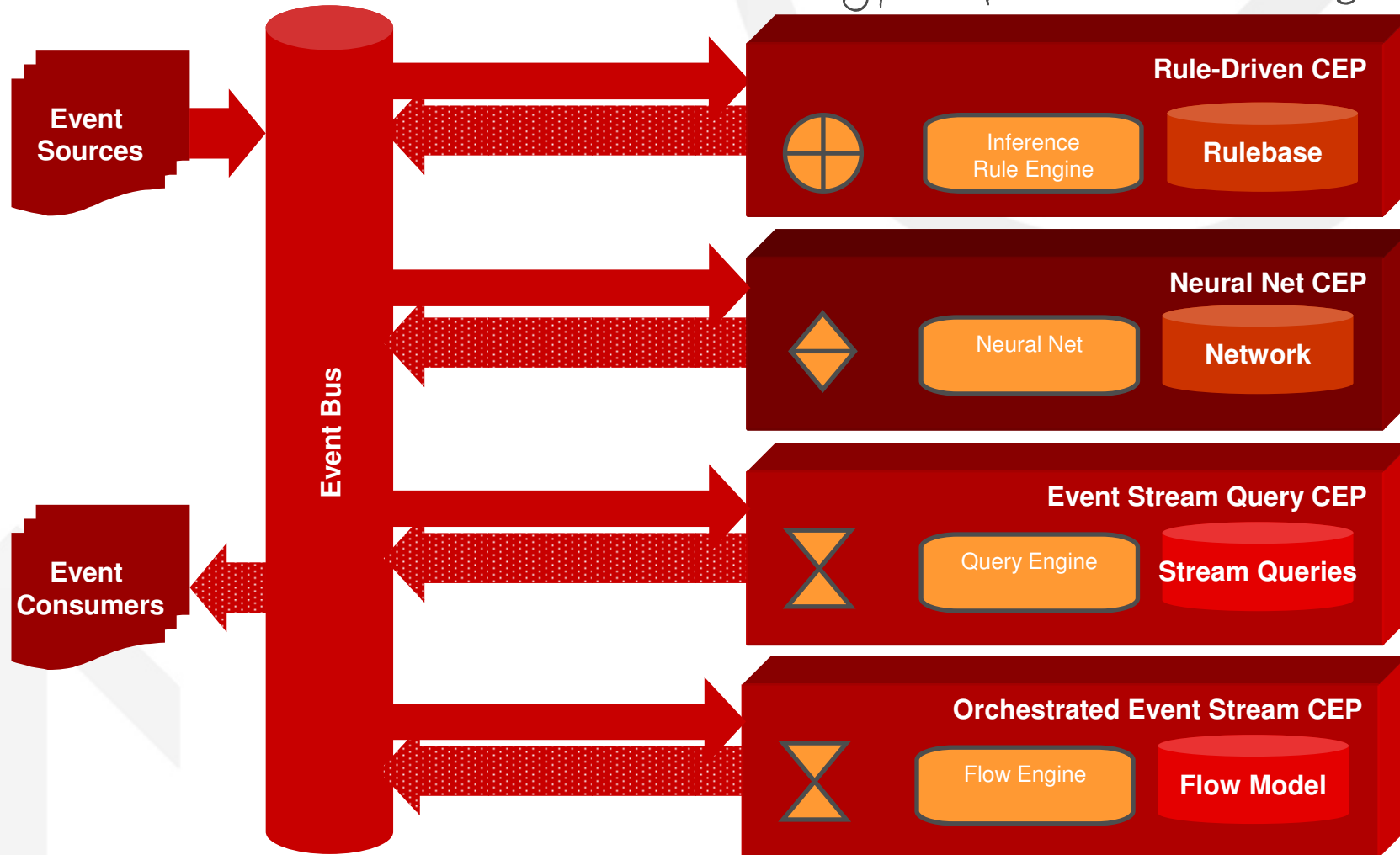
# CEP-Related Standards



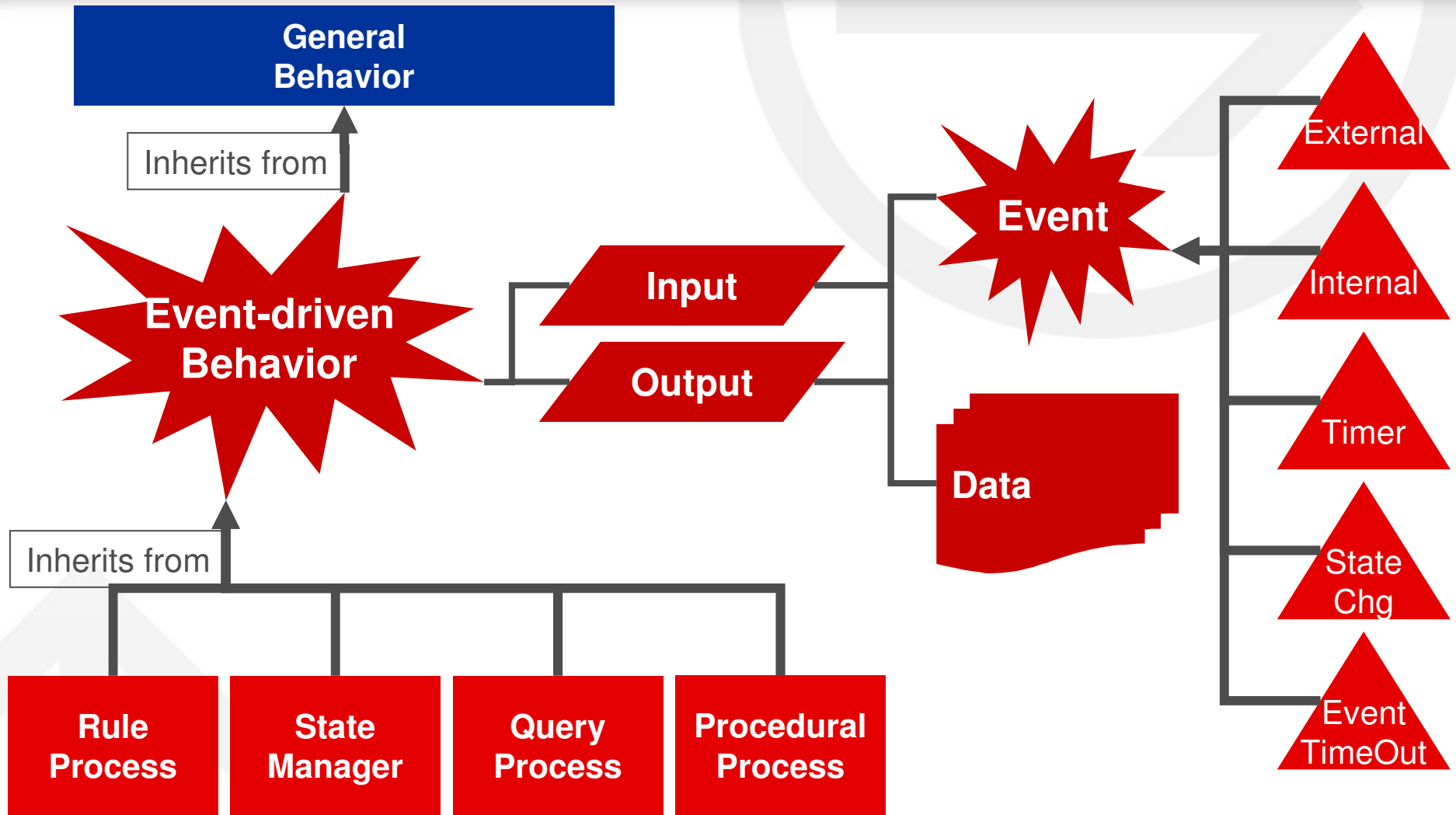
# Example CEP Technologies

Event Services

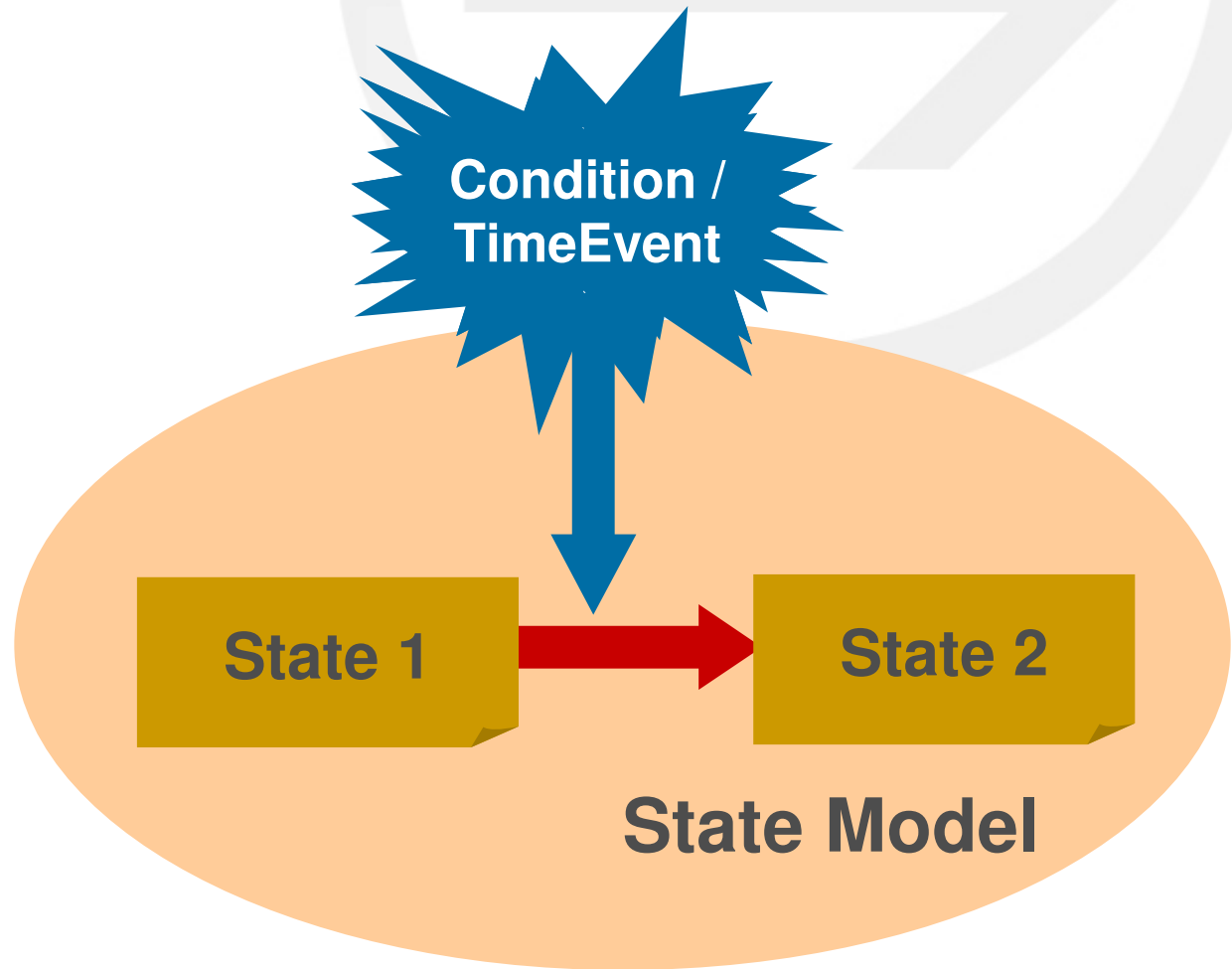
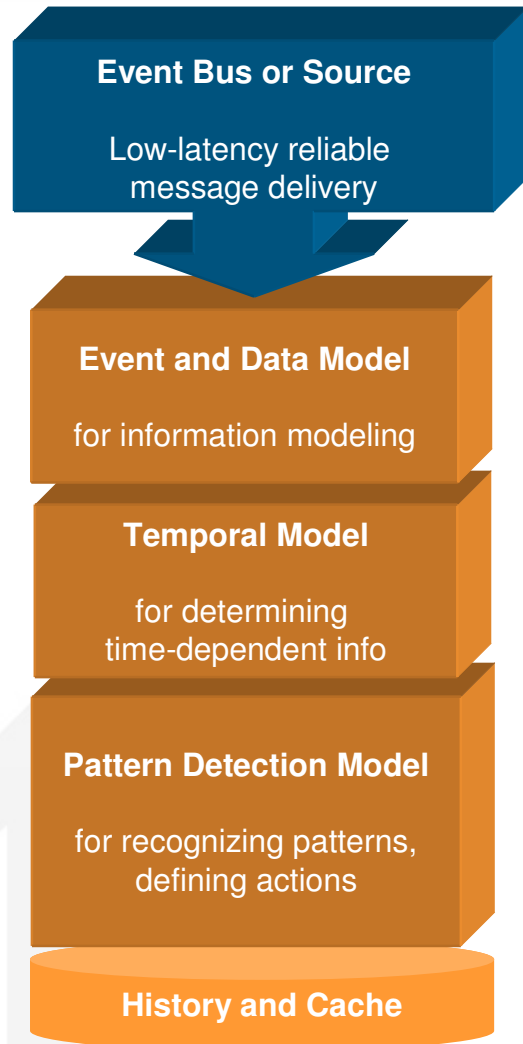
Types of CEP Processing



# Sample Event Processing Metamodel



# CEP Behavior: State-oriented



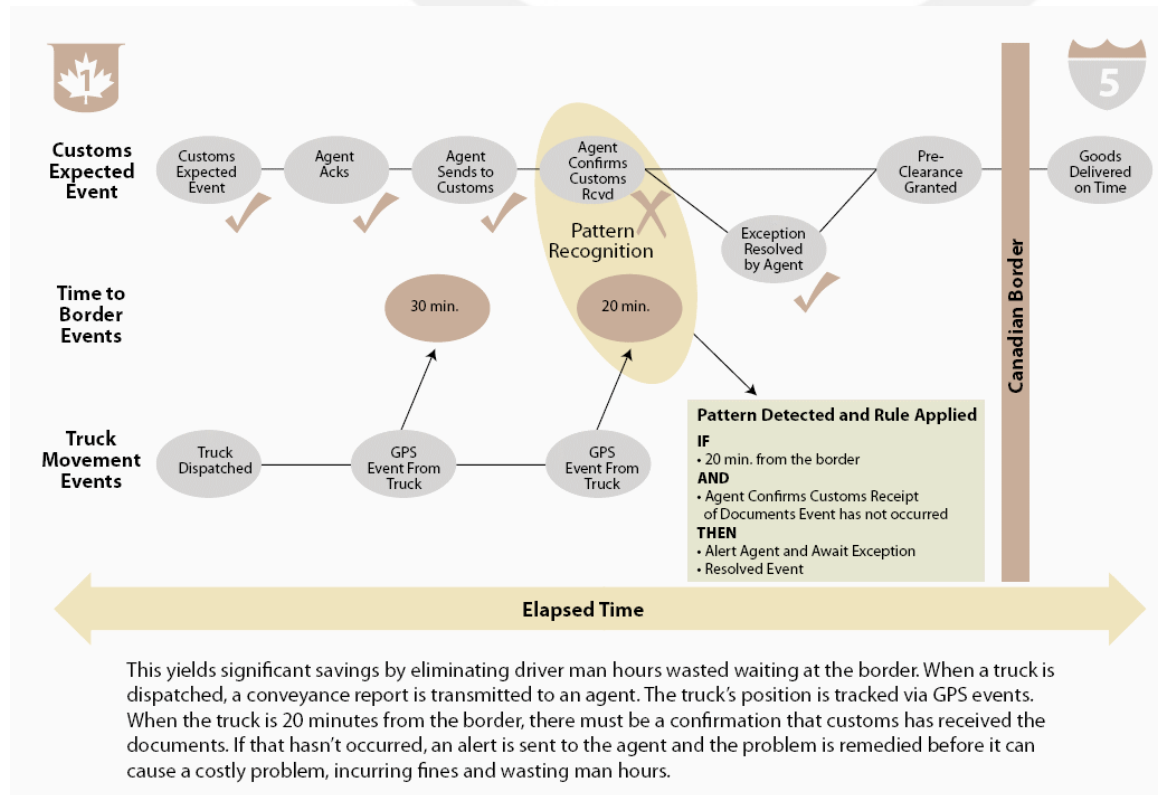
# State Model / Process Flow CEP Agent features

## 1. Visual modeling metaphor

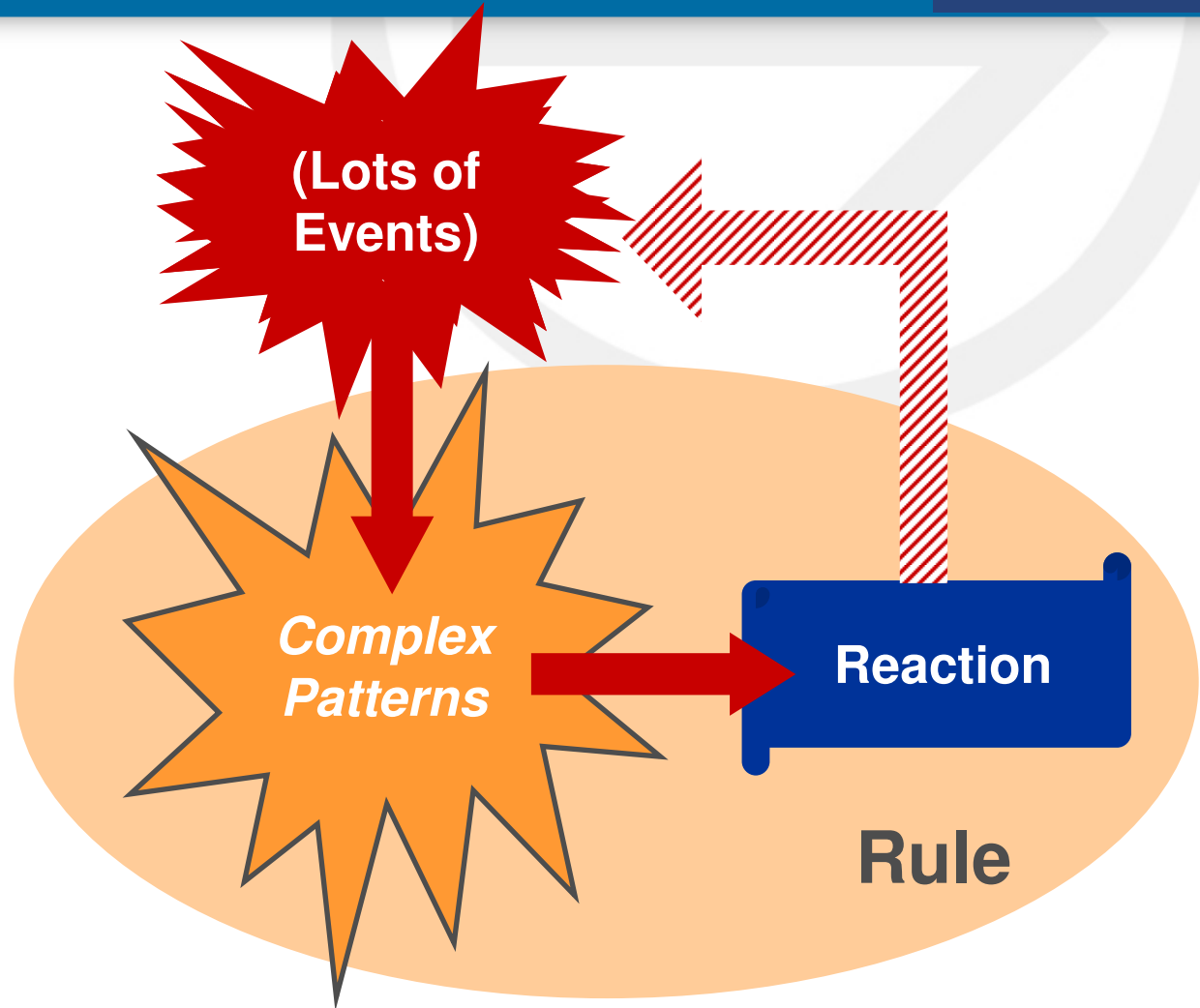
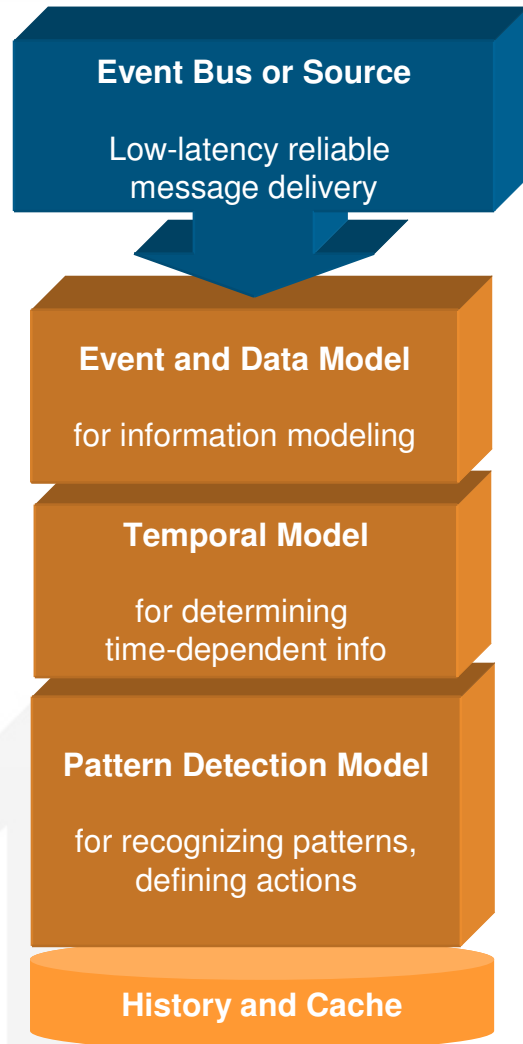
- State diagram / flow diagram is simple to follow

## 2. State / flow transitions can be time-related

- Can model missing events through time-outs etc



# CEP Behavior: Rule-oriented



# Inference Rule CEP Agent features

## 1. High performance pattern matching

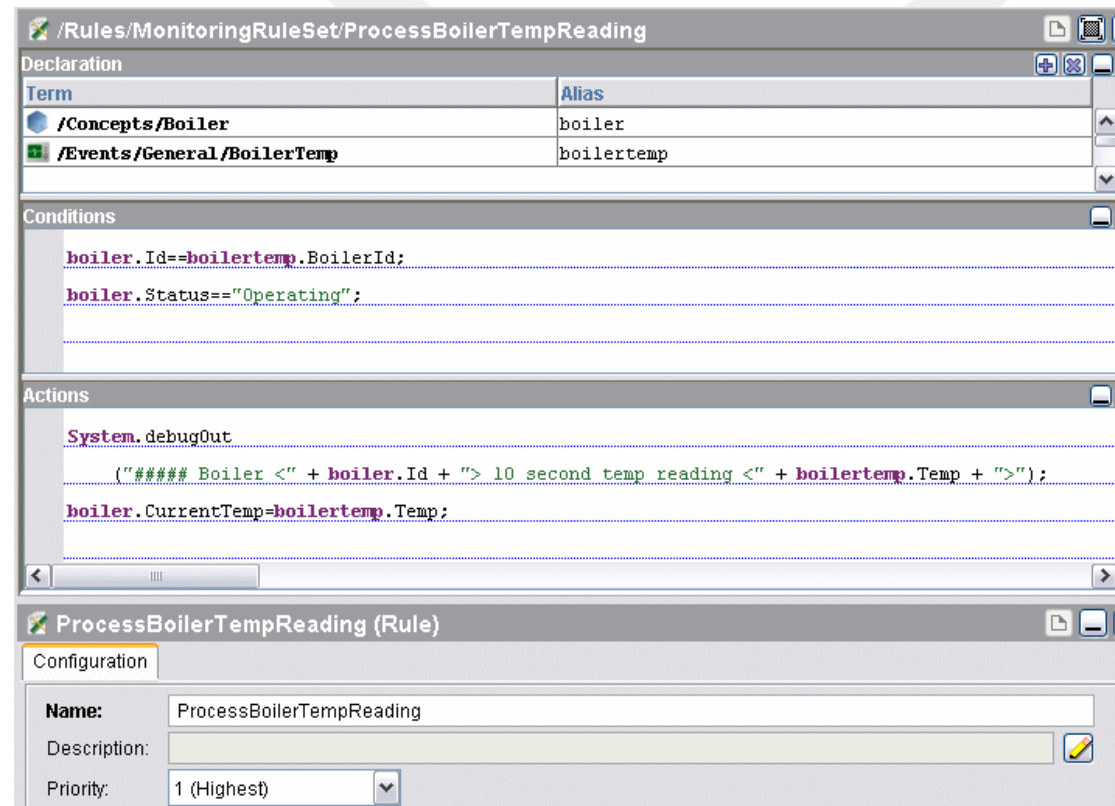
- Rete algorithm determines rules that are executable based on underlying data changes

## 2. Declarative + Inferencing

- Rules defined in terms of classes: can be relevant for any # instances
- Rules' actions can cause other rules to fire automatically

## 3. In-memory

- Limited only by JVM / process memory



The screenshot displays a rule editor window titled '/Rules/MonitoringRuleSet/ProcessBoilerTempReading'. It is divided into several sections:

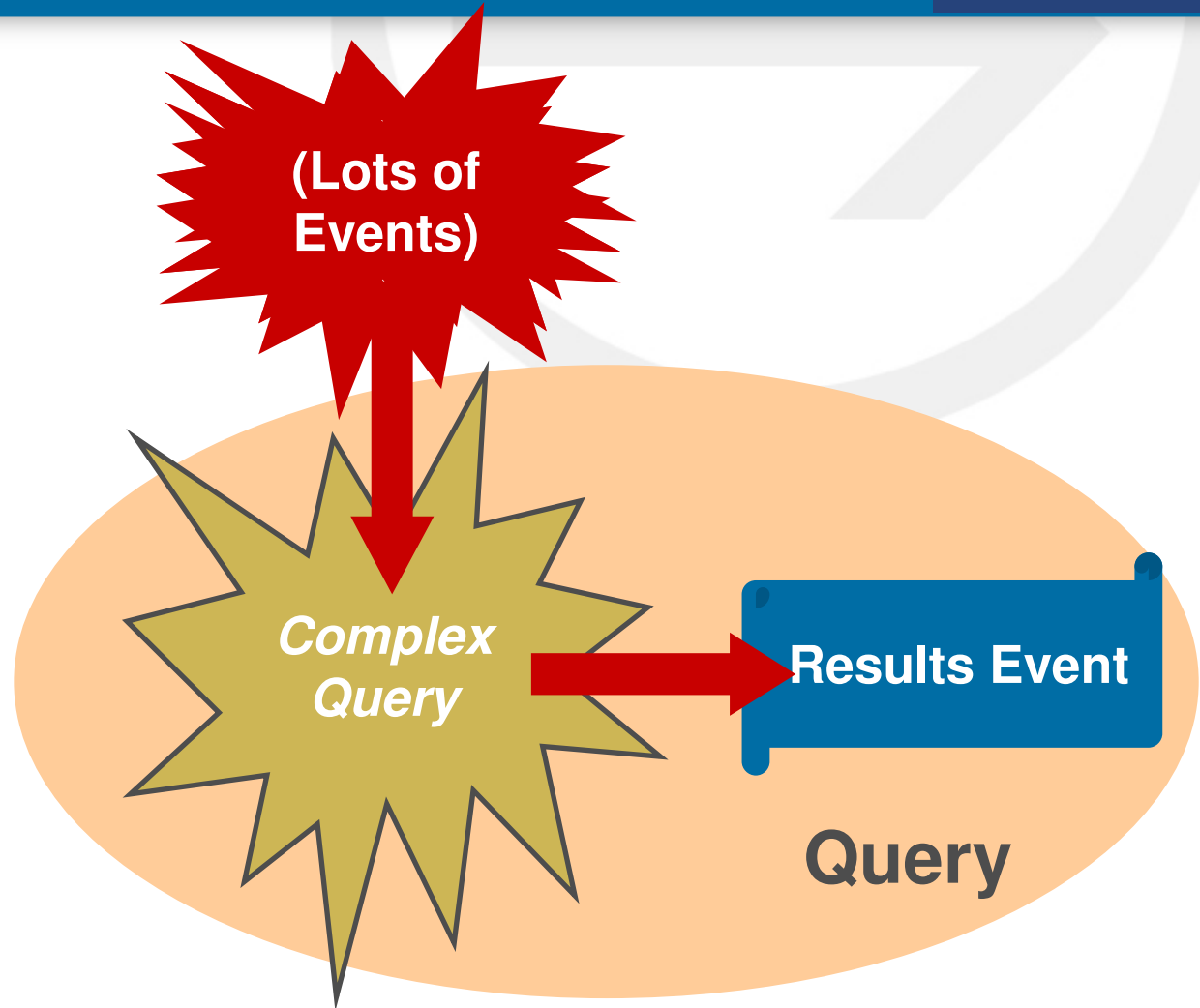
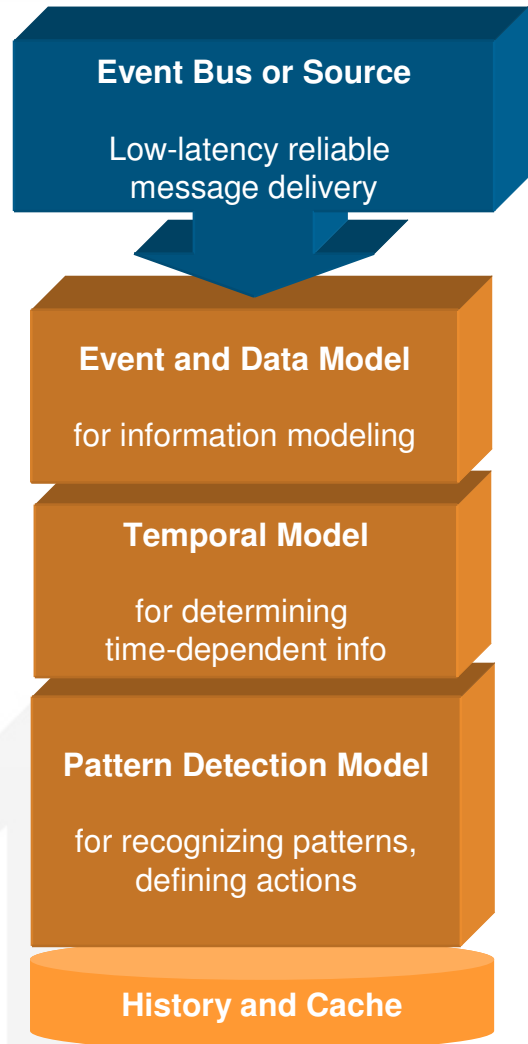
- Declaration:** A table listing terms and their aliases.
 

Term	Alias
/Concepts/Boiler	boiler
/Events/General/BoilerTemp	boilertemp
- Conditions:** A list of logical conditions:
 

```
boiler.Id==boilertemp.BoilerId;
boiler.Status=="Operating";
```
- Actions:** A list of actions to be performed:
 

```
System.debugOut
("#### Boiler <" + boiler.Id + "> 10 second temp reading <" + boilertemp.Temp + ">");
boiler.CurrentTemp=boilertemp.Temp;
```
- ProcessBoilerTempReading (Rule) Configuration:** A form for rule configuration.
  - Name:** ProcessBoilerTempReading
  - Description:** (Empty field)
  - Priority:** 1 (Highest)

# CEP Behavior: Query-oriented



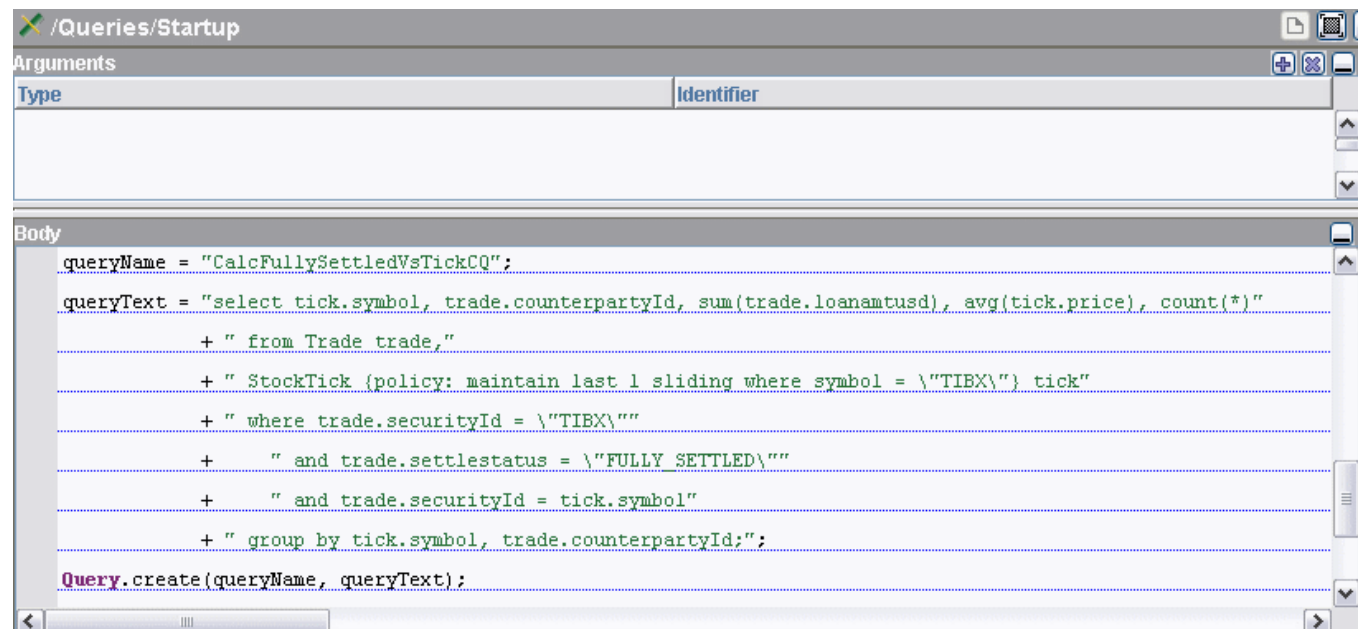
# Query CEP Agent features

## 1. Common query language

- Usually SQL-based – widely used language
- May be in-memory, in-file or both
- Can include query optimizers

## 2. Continuous

- Extensions usually support time windows for the query to operate over



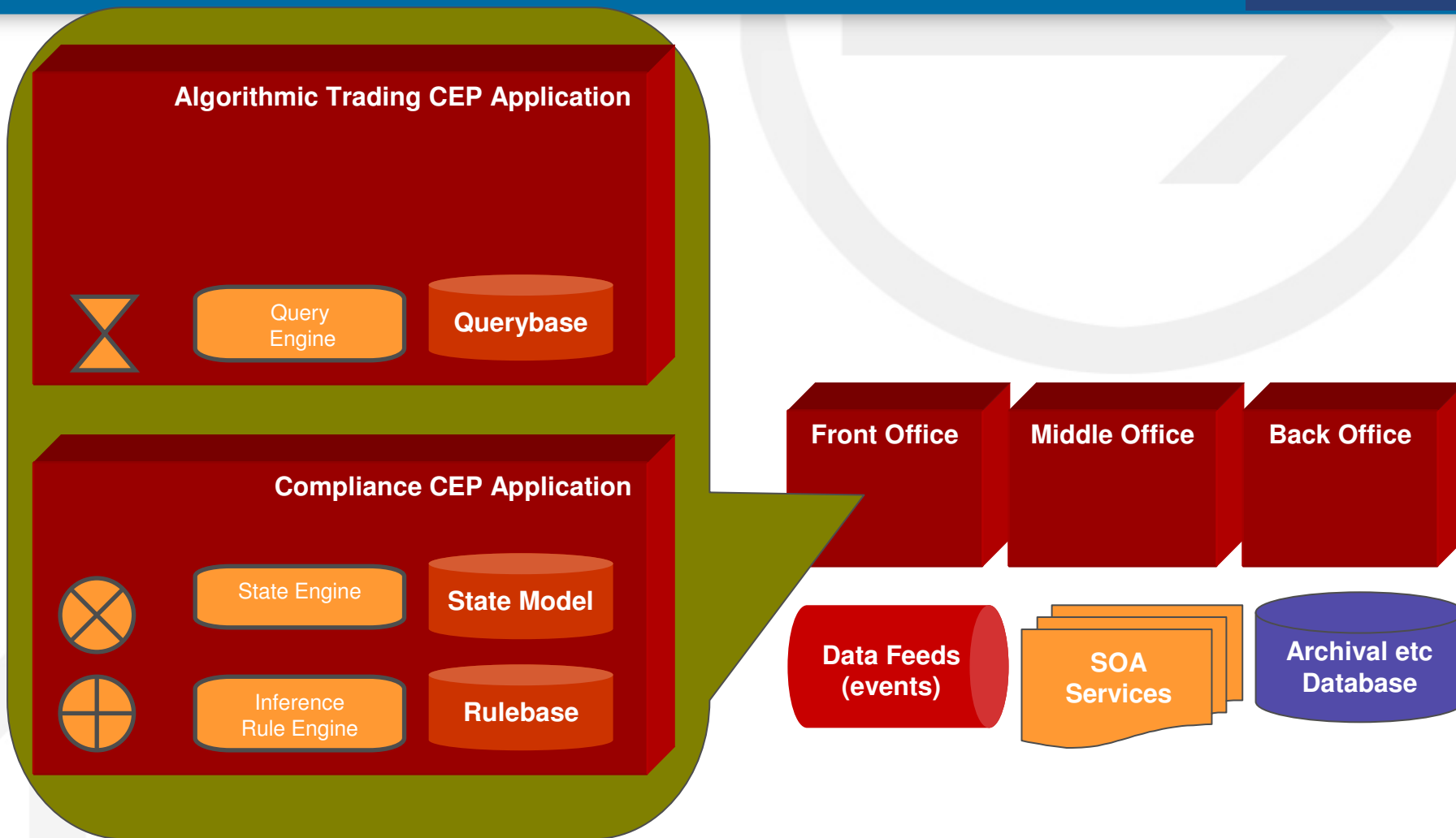
```
queryName = "CalcFullySettledWsTickCQ";
queryText = "select tick.symbol, trade.counterpartyId, sum(trade.loanamtusd), avg(tick.price), count(*)"
            + " from Trade trade,"
            + " StockTick (policy: maintain last 1 sliding where symbol = \"TIBX\") tick"
            + " where trade.securityId = \"TIBX\""
            + " and trade.settlestatus = \"FULLY SETTLED\""
            + " and trade.securityId = tick.symbol"
            + " group by tick.symbol, trade.counterpartyId;";
Query.create(queryName, queryText);
```

## ■ Examples

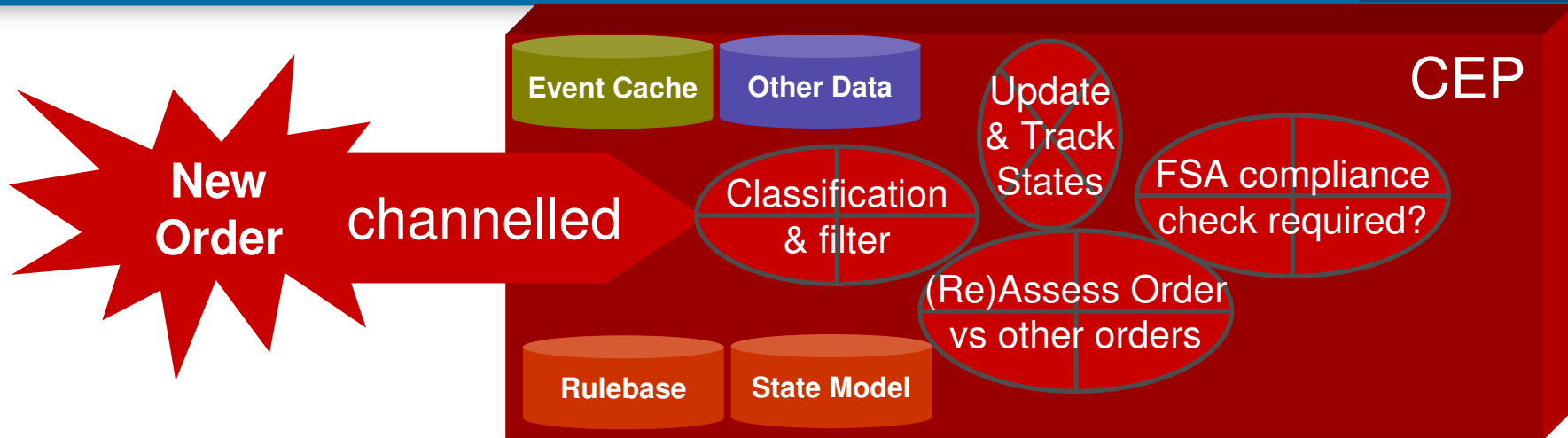
# Typical Business Situations for CEP

Detected Business Situation	Resulting Situation-Decision
User X is behaving suspiciously (high likelihood of fraud)	Investigate for fraud manually
Subcomponent delivery Y is slightly late	Issued an automated reminder to supplier
Customer Y payment for policy P is very late	Alert Customer Agent
Orders for product Z are up >20%	Alert manufacturing and marketing

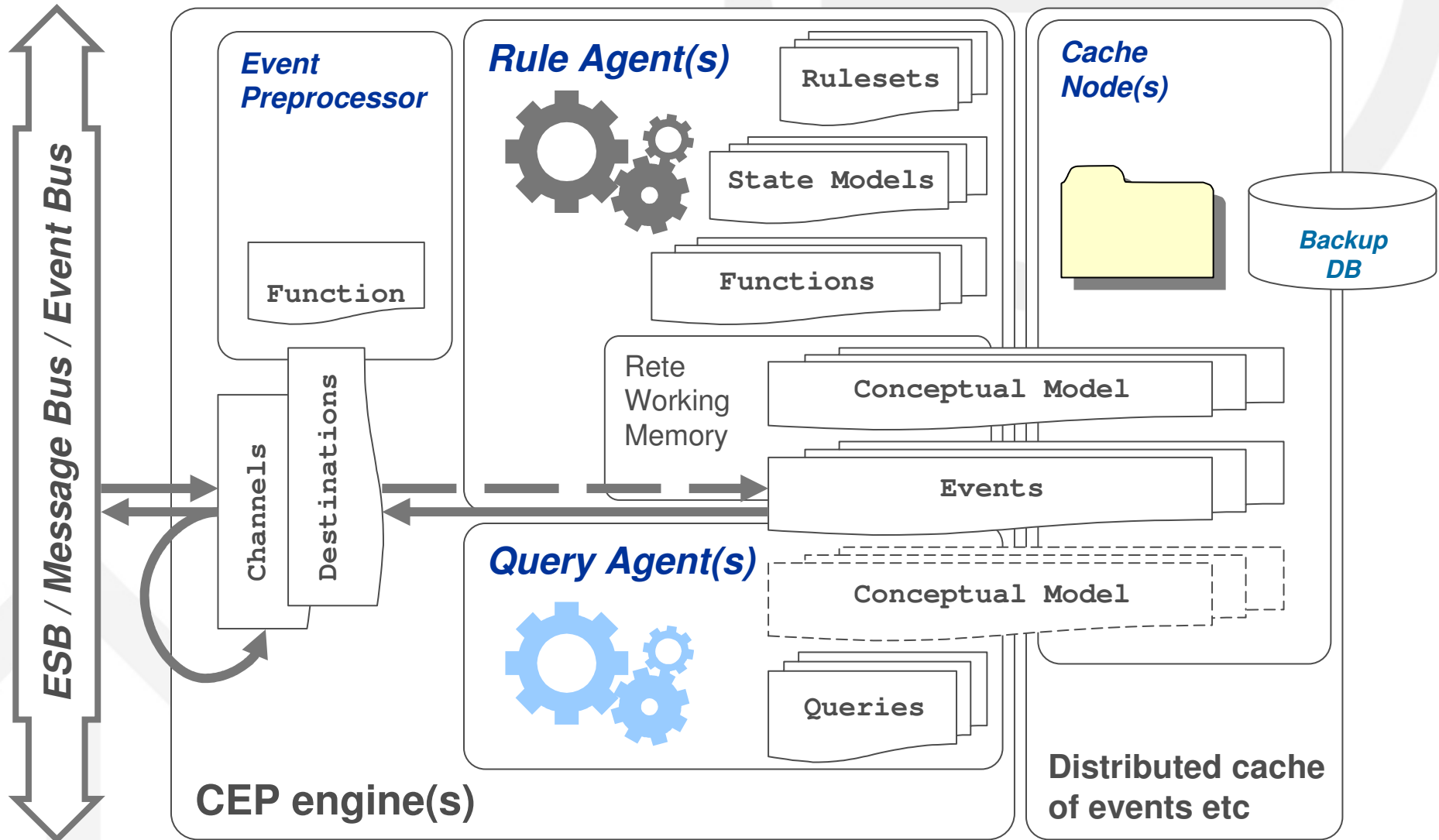
# CEP in Action: Investment Banking



# CEP Processing



# Example CEP Product Architecture



## ■ “Advanced” CEP

# “Advanced” CEP defined in many ways

## ■ Intelligent CEP

- Adaptive
- Learning
- Logic
- AI

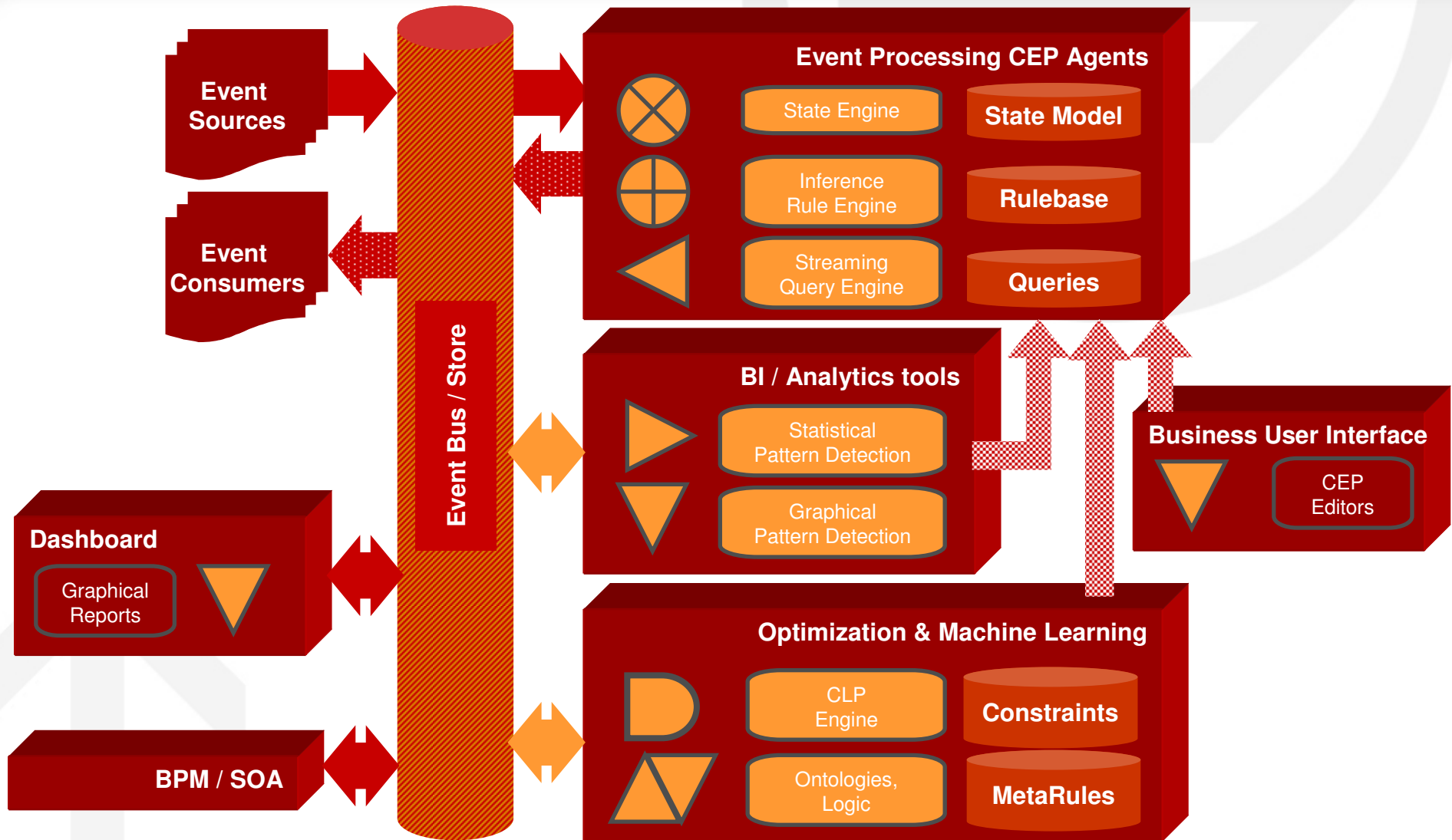
## ■ Semantic CEP

- Ontologies + Logic
- Text / language interpretation

## ■ Multiple CEP

- Including all types of data processing paradigm  
(transactional, CLP, inference, mathematical methods, ...)

# Advanced CEP Infrastructure



# Advanced Patterns & Event Behaviors

- **Many EP apps fit the standard CEP patterns:**
  - Filter interesting rules
  - Detect predefined patterns / state changes
  - Update data / invoke processes and services based on business rules and high level events
- **Advanced EP:**
  - Apply interesting statistical functions to event data to detect new / complex trends
  - Apply different algorithms to event data
  - Modify parameters used in other rules (“metarules”)

Term	Alias
/Model/Seat	seat
/Model/Guest	guest
/Model/Guest	rightGuest
/Model/Context	context

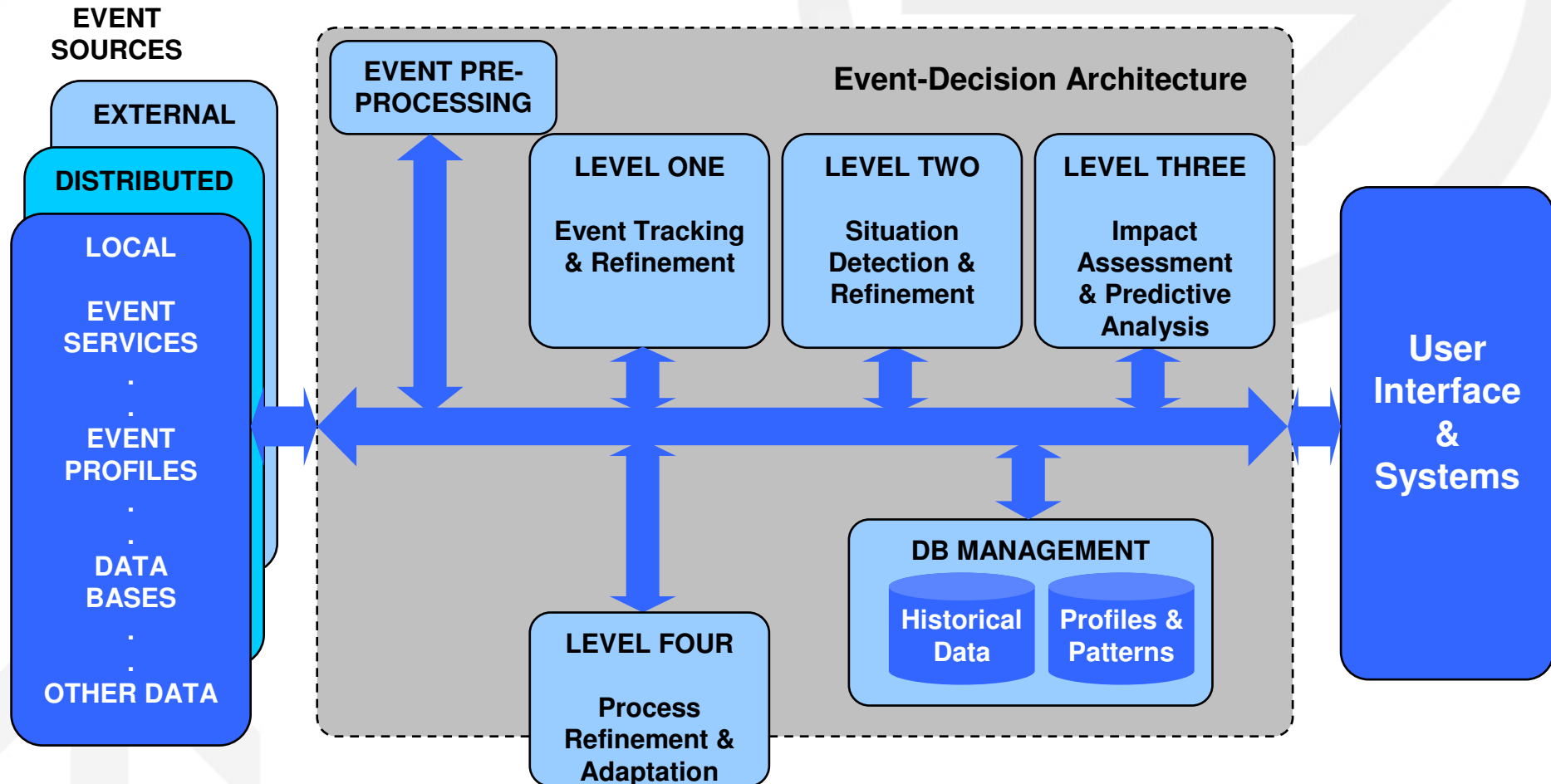
```
seat.guest == guest;
guest.sex != rightGuest.sex;
checkHobbies(seat, rightGuest);
notAssigned(seat.leftSeat, rightGuest);
context.status == "processing";

Seat rightSeat = Seat(null /*extId String */,
                      rightGuest /*quest Model.Guest */,
                      seat /*leftSeat Model.Seat */,
                      seat.position+1 /*position int */);

//System.debugOut("Search Path: " + printPath(rightSeat));

//check if we are done
if(rightSeat.position == context.numGuest) {
    Seat firstSeat = Instance.getById(context.firstSeat);
    if(checkHobbies(rightSeat, firstSeat.guest)) {
        //check with the quest in first seat
        firstSeat.leftSeat = rightSeat;
        context.endTime = DateTime.now();
        context.status = "end";
    }
}
```

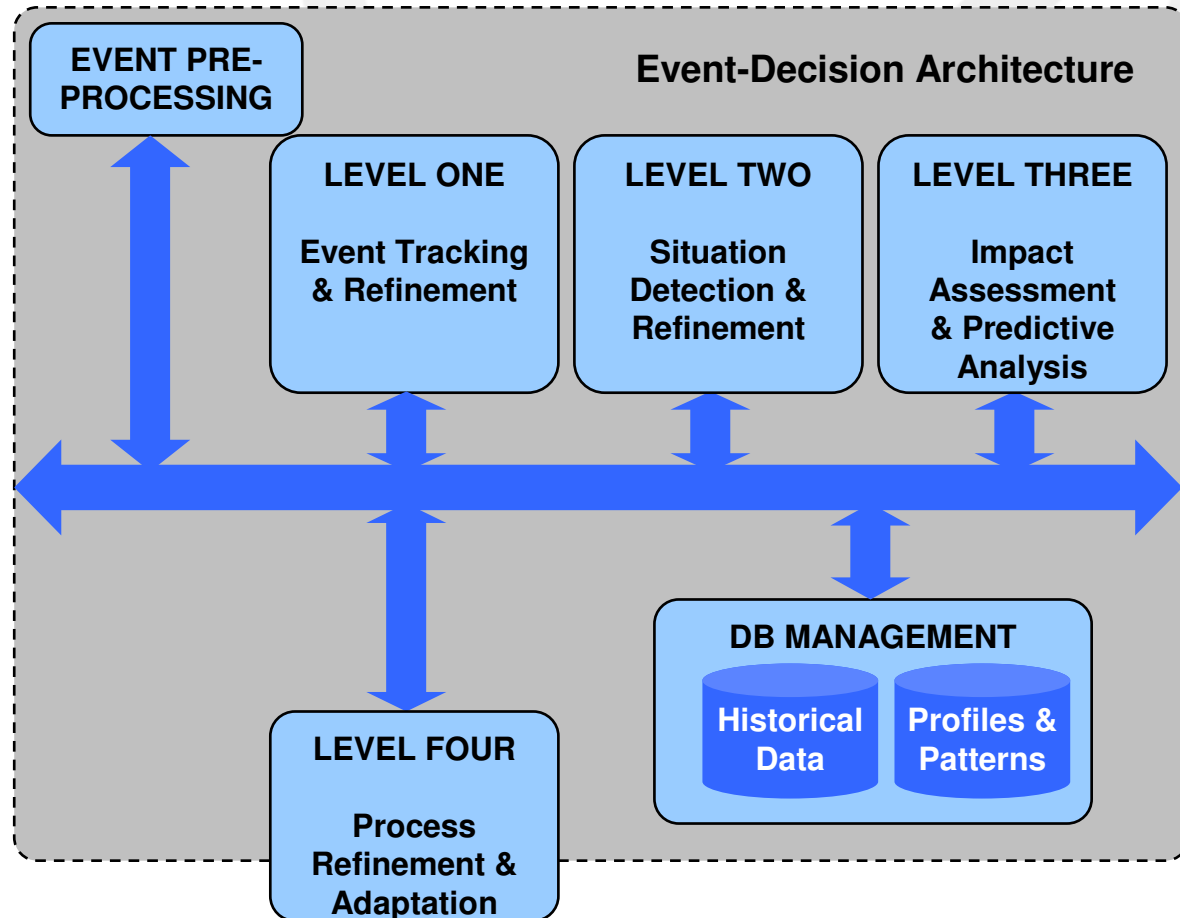
# “Event-Decision” Architecture



-- Adapted from JDL Steinberg, A., & Bowman, C., Handbook of Multisensor Data Fusion, CRC Press, 2001

# Self-Modifying “Event-Decision” Rules

- What are the variables that can be adjusted in real-time to optimize system performance?



# Pre-Processing Event Filtering Rules

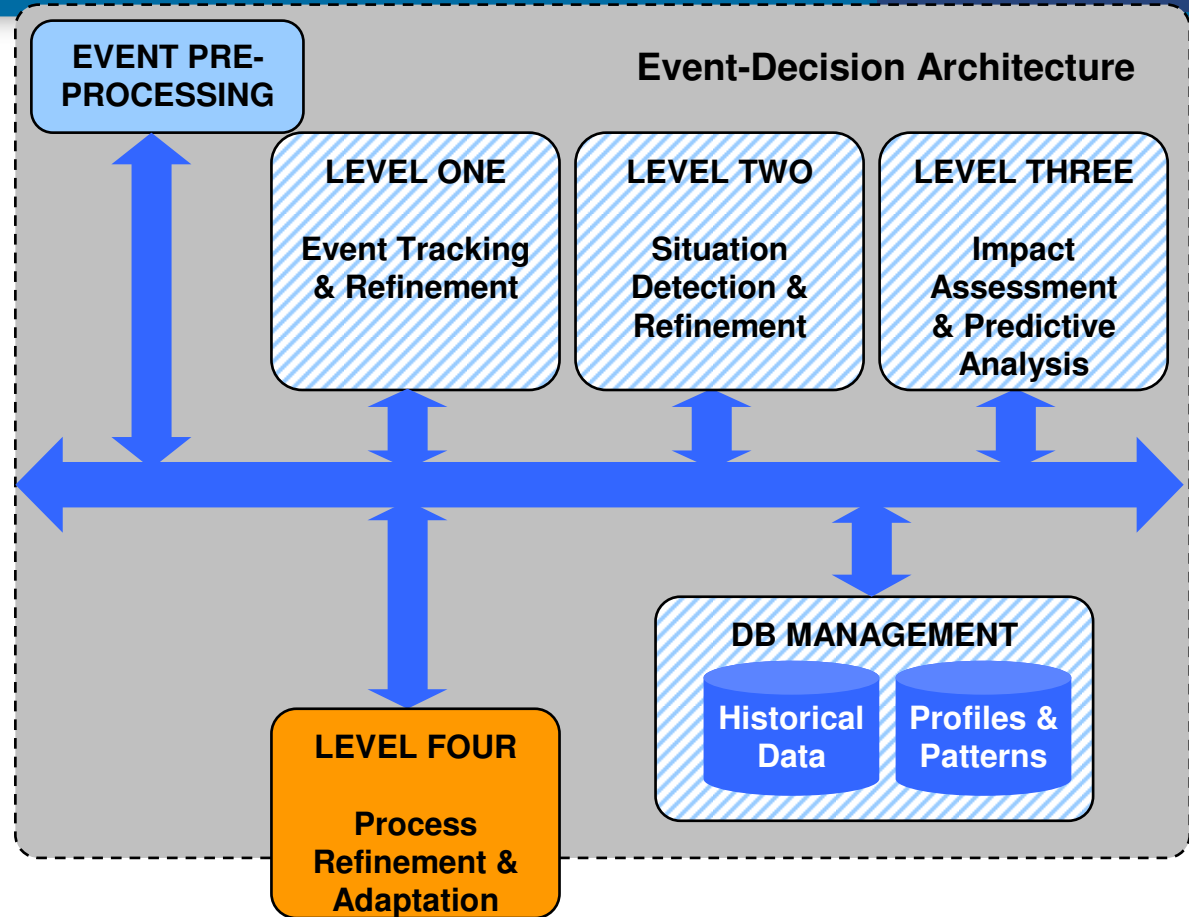
```
If RFID event for
product X
Then
monitor, else
ignore
```

Becomes

```
If RFID event for
product in list Y
where cost > Z
Then monitor, else
ignore
```

Updated by

```
If average loss increase
for all products in Y > 2%
Then reduce Z by 5%
```



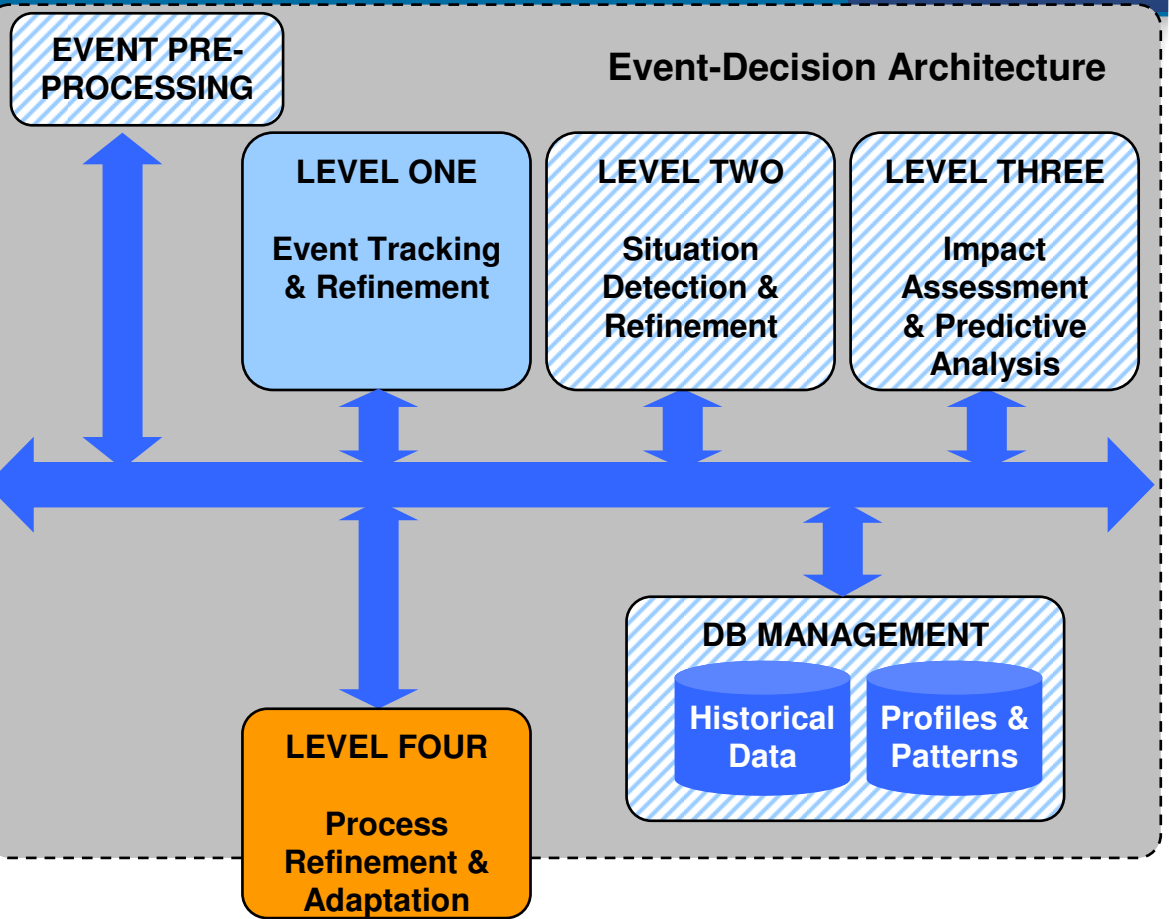
# Event Tracking and Refinement Rules

If drug class X  
 and dose > 200ml  
 Then  
 move to monitored  
 drug state

Becomes

If drug class X  
 and dose > Y ml  
 Then  
 move to monitored  
 drug state

Updated by



If clinical negative events for  
 drug class X increase  
 Then reduce Z by 10ml

# Event Tracking and Refinement Rules

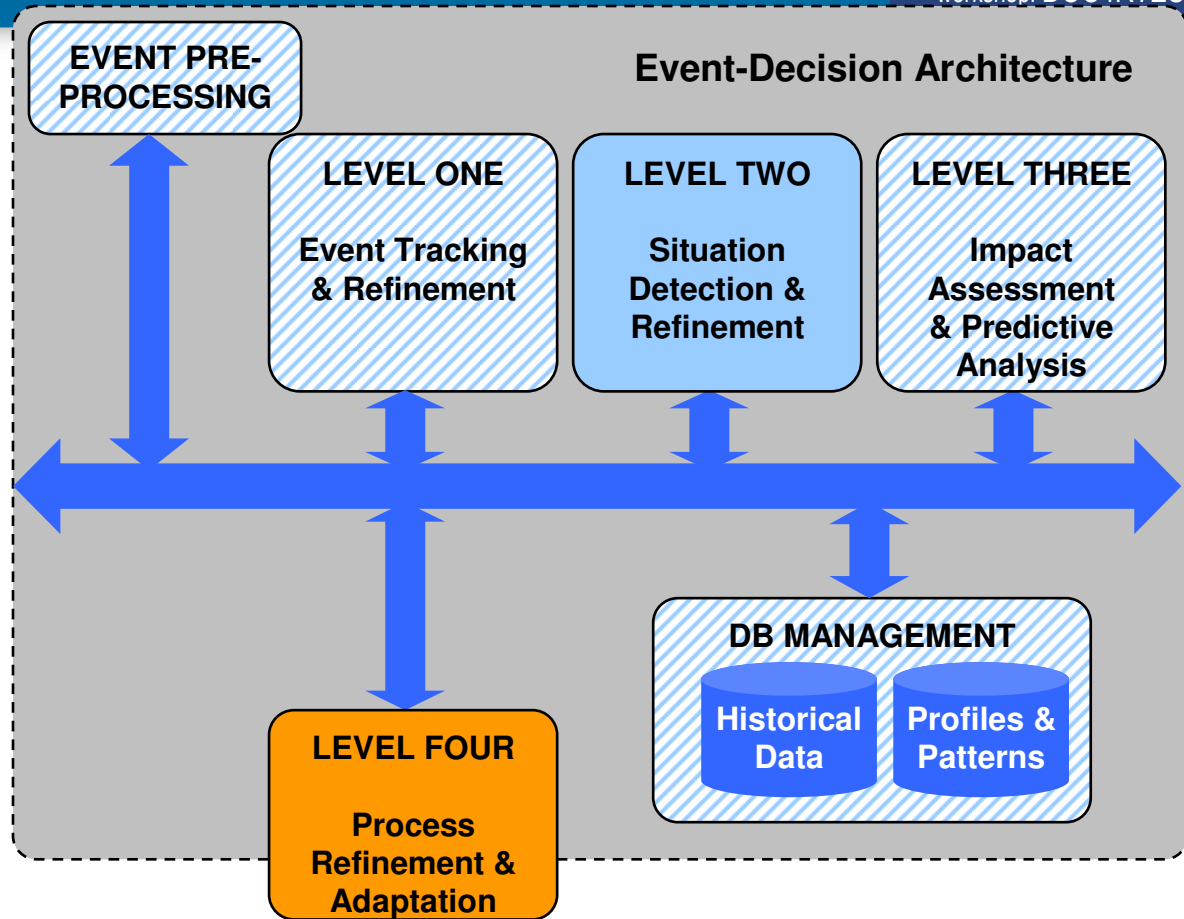
```
If bag X is not on
prescribed flight
at (depart - 20)
Then
move X state to
MissedFlight
```

## Becomes

```
If bag X is not on
prescribed flight
at lastBagTime
Then
move X state to
MissedFlight
```

## Updated by

```
If flight NOT international
Then set lastBagTime to
carrier's min( DoorCloseTime)
```



# Event Tracking and Refinement Rules

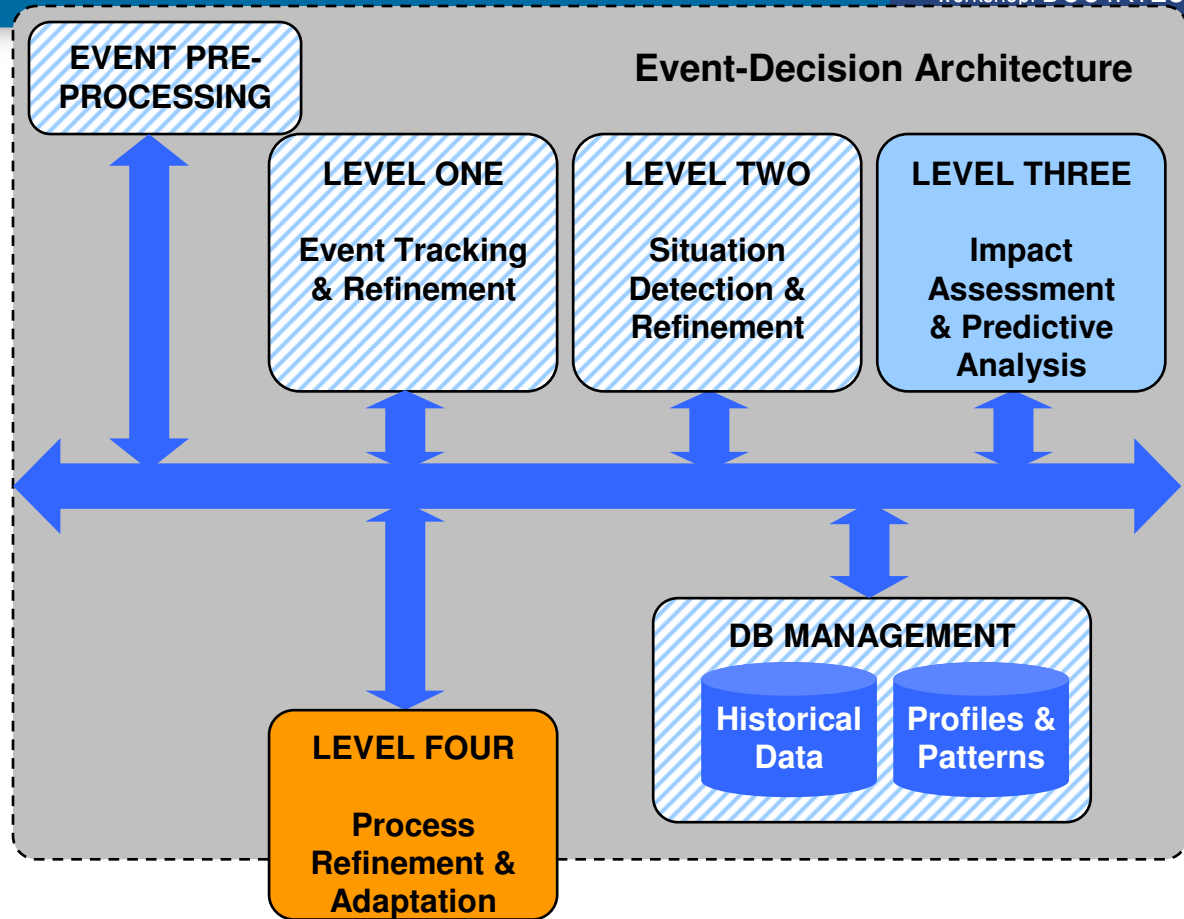
```
If  
  product.ShipDelay  
  > 1 days  
Then  
  contactLegal
```

## Becomes

```
If  
  product.ShipDelay  
  > contract.SLA  
  MaxDelay -  
  AllowedShipLag  
Then  
  warnLegal
```

## Updated by

```
If contract.customer.status = Hi  
Then set AllowedShipLag to 2  
  days
```



- **Needs constraints**
  - Eg Cannot reduce discount to  $<0$  or increase above  $>25$
  - Can handle as “change events” and rules to test...
- **Difficult to test**
  - May be based on statistical functions – implies complex test regimes (or test-specific rules)
- **Complex to prove ROI / value**
  - End-user may not be able to source or validate the advanced rules
- **Requires statistical function libraries / analytics**

# Other sources for “advanced rules”

- **Uncertainty**
  - Scoring
- **Generating rules**
  - Machine learning
  - Predictive Analytics
  - Reasoning + Ontologies
- **Other types of rules**
  - Constraint Logic Programming

- Simple technique to handle “variable” decisions
- Rules update a score
- Example: insurance scoring
- Typically handled in a special ruleset (or decision table)
- Good as a KPI in a scorecard
- Typically used with an aggregation rule

Object Property	Condition	Score Effect
Age	<18	-10
Age	19 to 26	-15
Age	27 to 49	+5
Age	50 to 69	0
Age	70+	-5

# Machine Learning

- Given a set of data, deduce classification patterns and hence rules
- Requires sophisticated algorithms

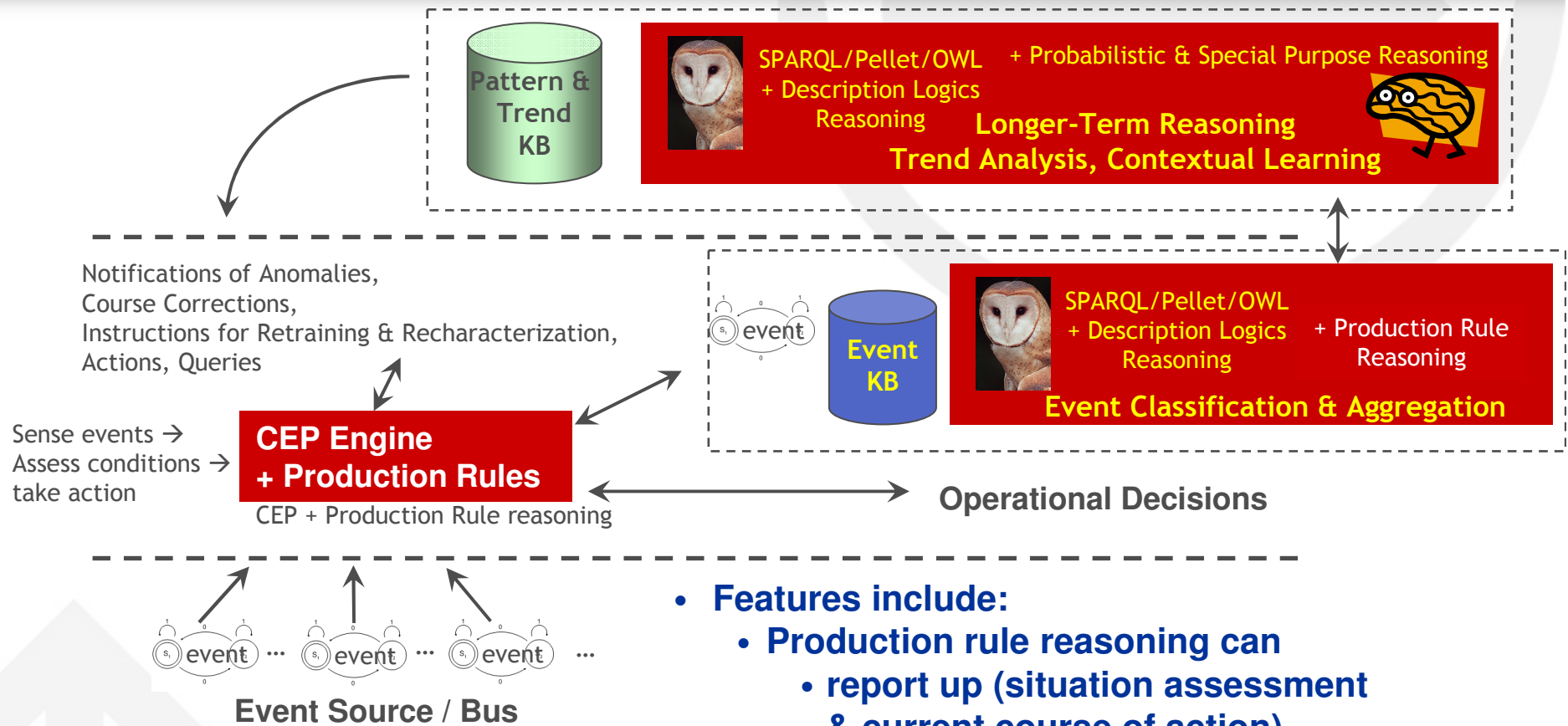
data				result
A	A	A	A	1
A	B	A	B	2
B	A	B	A	3
other	other	other	other	4

- **Analyze data to deduce segmentation breaks for tasks like customer classifications**
  - Eg: Which customers should be offered what interest rate to maximise profit?
- **Typically using specialist data mining tools**
  - Exports decision tree, rules etc in varieties of PMML
- **Overlaps with BI (eg custom reports on historic data)**
- **Analytical functions may also be mapped to a ruleset in CEP for real-time analytics**

- **“Semantic Event Processing”**
- **Use Semantic Web technologies to augment CEP**
  - Textual news etc analysis
  - Use of deeper ontology relationships
- **Example components**
  - OMG Ontology Definition Metamodel ODM joins W3C OWL to UML concept models
  - OWL, RDF, RDFS for terminology, relationships
  - Logic languages/rules to reason about truth over event types and metadata

# Example: Semantic Technology to Refine CEP

## Semantic Networking Event Monitoring Architecture



- **Features include:**
  - **Production rule reasoning can**
    - **report up (situation assessment & current course of action)**
    - **report laterally (situation assessment, & sensed changes, etc.)**
    - **report down (initiating actions, querying)**
  - **Adaptive capabilities are possible at all levels**

-- courtesy of Sandpiper Software

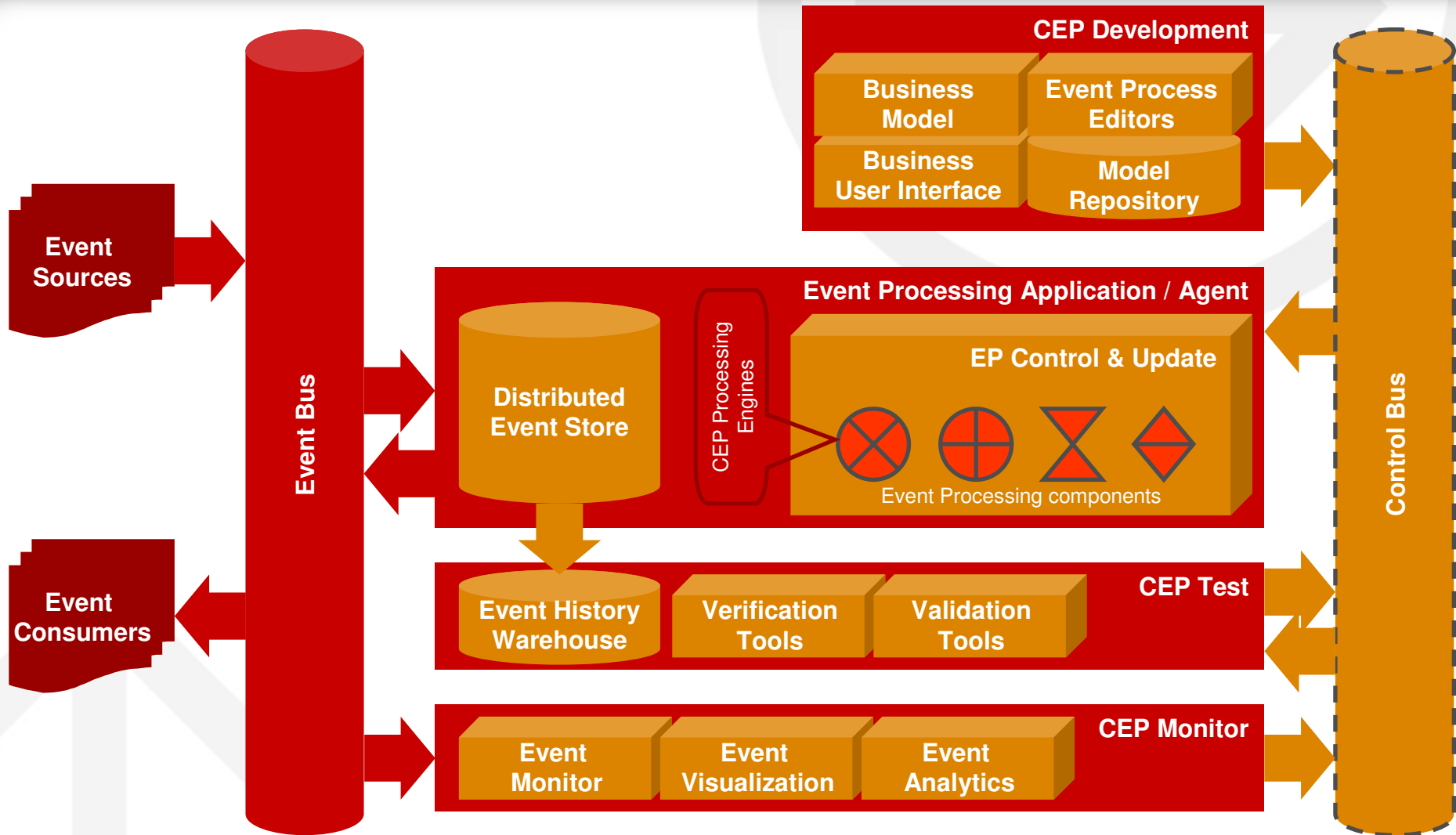
- **Constraint rules for systems**
- **Constraint solver to find best values (eg optimize price)**
  - With response time as a system constraint!
  - Goal-driven
- **Uses:**
  - Maximizing value of inventory
  - Scheduling the best routes for trucks
  - Maximizing probability for SLA achievement

## ■ The End

## ■ Q & A

## A. Appendices & Back-up Information

# Appendix: Generalized Architecture for CEP



## Appendix: Useful web resources

- **Event Processing Technical Society EPTS**  
[www.ep-ts.com](http://www.ep-ts.com)
- **Luckham's web site**  
[complexevents.com](http://complexevents.com)
- **Various vendor blogs (reference from complexevents.com)**