DYNAMIC
Complex Event Processing
Not Only the Engine Matters!

Bernhard Seeger
Universität Marburg
Motivation

reactive monitoring of time-critical business processes

• predictions about the near future and recommendations for action
Situations of Interest

![Diagram showing the relationship between Time, Impact, Reaction Costs, and Options.](Image)

- **Impact**
- **Reaction Costs**
- **Options**

© Bernhard Seeger
Agenda

- Motivation
- Review of CEP
- Dynamic CEP
  - Requirements
- Conclusion
2. Overview of CEP

- CEP application
  - Registration of event sources
  - Definition of EPAs (Event Processing Agents)
  - Registration of Event Sinks
Comparison CEP ↔ DBMS

**DBMS**
- Persistent data
- Flowing queries
- …
- Dynamic
  - Insertions and Updates of data
- Data independence
- Data quality
- Standards

**CEP**
- Persistent Queries
- Flowing Data
- Temporal Data

© Bernhard Seeger
Static CEP

- **Static Approach**
  - Signature-based EPA
  - Deployment of a fixed system
  - Changes of the system
    - offline
    - purely manual

- **Observation: CEP is highly context-sensitive**
  - Temperature depends on season
  - Network traffic patterns (weekdays – weekend)

- **Fast changes of contexts**
3. Dynamic CEP

- Key Features
  - Event/EPA independence
  - Event store
  - Model store
  - Dynamic EPAs
3.1 Event/Query Independence

Requirements

- If new event sources are inserted
  ➔ no modifications of EPA
- If new DEPA are inserted
  ➔ no modifications of event sinks
Matchmakers

- **Basic idea**
  - Virtual sensors/DEPA
    - Indirect connections through continuous queries on metadata
      “Return all temperature sensor data 10 km around TU München”

- **Input Matchmaker**
  - New sources at runtime without modifications of DEPA

- **Output Matchmaker**
  - New DEPA at runtime without modifications of sinks
3.2 Dynamic EPAs

- **Goal**
  - Detection of abnormal behavior in event stream

- **Change of EPAs at runtime**
  - Not only a performance issue
  - Impact on the semantics of queries
    - Day mode → night mode

- **Questions**
  - When should a DEPA be changed?
  - How should a change be performed?
Event Store

- Persistent management of the history of events.
- Append-only database (XXL-AO)
  - Optimized for fast writes
    - 2 Mio/s using a single disk
  - Queries
    - Efficient support of temporal predicates
    - If possible also other types of predicates
  - Fast garbage collection and compression of outdated events

© Bernhard Seeger
Model Store

- Management of models for describing normal behavior
  - State-based models
    - Average
    - Histograms
  - Process-based models
    - Markov models

- Patterns of models
  - Parameters still need to be adapted for a specific context
Model Patterns → Model Instances

- Derive instances from patterns
  - Learning the best parameter setting of these models from the past.
    - number of parameters should be limited
- Monitoring the quality of model instances
Simulations

- Running of EPA in a sandbox using real data (from the event store)

- Benefits
  - Test and debug EPA
  - Support of what-if analysis
  - Adaption of DEPA
    - Identify points where one DEPA has to be replaced by another one.
Actions

- Current CEP systems don‘t care about actions
- Need actions for reactive CEP
  - How to prevent detect-react-cycles?
  - Avoid contradictive actions?
  - Provenance
    - Event store
    - Reproducibility of results
Quality of EPA

- Data quality is a big issue in databases
- What about EPA quality in CEP?
  - Set of EPA is the most important asset!
    - Need research on this important topic
  - Prerequisite for semi-automatic generation of queries
    - Ideally: Minimal, but complete set of queries
Standardization

- Well covered in databases, but the CEP area is still too diverse
  - vendor locking
  - no federation of CEP engines

- Java Event Processing Connectivity
Conclusions

- **Dynamic CEP**
  - Substantially more than a CEP-engine
  - Enhancements required in real CEP use-cases
    - Dynamic-enabled CEP
      - EPA independence
      - Quality Management of EPA
        - Event Store
        - Model Store

- **Current use-case for Dynamic CEP**
  - IT security: Anomaly management in Computer Systems using CEP Technology
Thanks

- This is common work with Bastian Hossbach

- Dieter Gawlick for our great discussions

- Our student team: Nikolaus Glombiewski, Andreas Morgen, Frank Ritter

- BMBF for funding ACCEPT