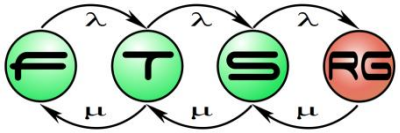
Komplex eseményfeldolgozás (CEP)

Gönczy László
gonczy@mit.bme.hu
Bergmann Gábor, Dávid István és az OptXware Kft. anyagainak felhasználásával



Tartalom

- Szabályalapú megközelítés felhasználása: komplex eseményfeldolgozó rendszerek
- CEP felhasználása
- Esettanulmány: CoMiFin
- Eseményfeldolgozás modell alapú tervezése

Kihívások

- Sok információforrás
  - „Szenzorok”
  - Felhasználói lépések szekvenciái
  - Logok
  - Külső szolgáltatások
- Sok esemény
  - Pl. ~százas nagyságrendű szervermetrika, százas nagyságrendű szerver
- Sok „érdektelen” esemény közt néhány minta
- Párhuzamos, online adatfeldolgozás szükséges
  - Hagyományos adatbázis alapú módszerek lassúak lehetnek
  - Egyszerre nem fér el minden esemény egy feldolgozóegység memóriájában
- Feladat: események feldolgozása és korrelációja
  - Kis késleltetéssel
  - Aszinkron módon
- Kérdés: mit figyeljünk?

CEP alapelvek

- „Komplex esemény”
  - Több elemi esemény összekapcsolása
- Tulajdonságok
  - Időzítések figyelembevétele (pl. csúszóablak)
  - Aszinkron működés
  - Oksági kapcsolatok, hierarchikus események
  - Korreláció
  - „Forward chaining”
- SQL-szerű query nyelvek
  - Pl. EPL: Event Processing Language
  - Feldolgozási folyamatba láncolható lépések
  - Event-Condition-Action
- Elosztott adatforrások
  - Adatbázisok, beérkező kérések, megfigyelt események, stb.
- Skálázhatóság
  - Cloud környezet

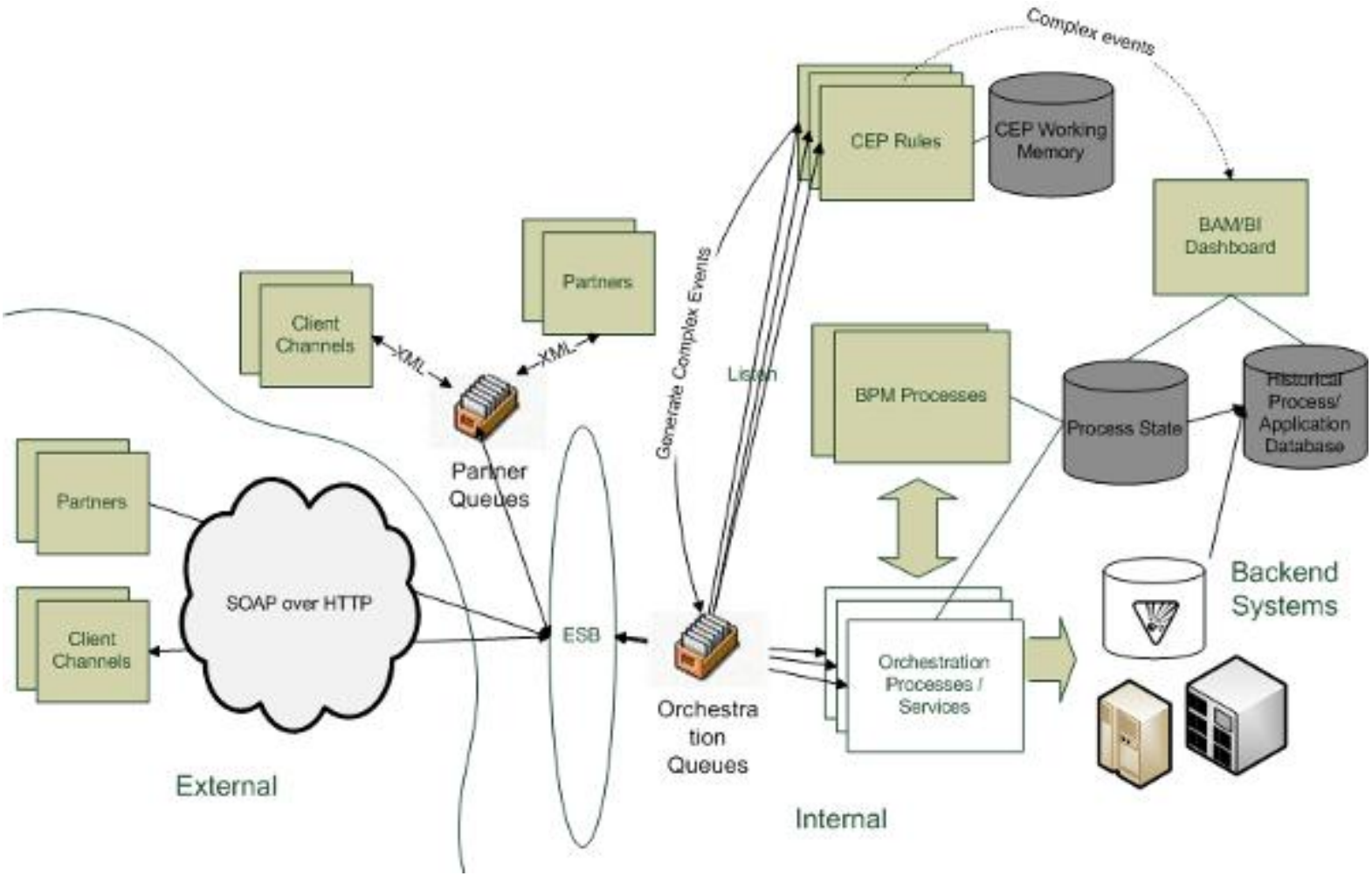
CEP alkalmazási területek

- Üzleti alkalmazások
  - Tőzsde, befektetések
  - „Treasury”
  - Kockázatkiértékelés
  - Hitelek árazása
  - Szállítmánykövetés
- „Business Activity Monitoring”
- Online visszaélések felderítése/megelőzése
  - Gyanús tranzakciók ellenőrzése
  - Fogadási adatok elemzése (pl. UEFA)
- Nagy IT rendszerek üzemeltetése
  - Komplex támadások felderítése
  - Metrika kiértékelés
- Biztonságtechnika
  - Pl. dDOS ellen
- http://www.complexevents.com/

CEP vs SzolgInt

- Hogyan kapcsolódik a szolgáltatásorientált rendszerekhez?
- Döntéstámogatás
  - ~szabálykiértékelés
- Monitorozó logika
  - Működés helyessége
  - KPI kiértékelés
- CEP lehet maga is egy szolgáltatás
  - Eseményeket küld → folyamatokat indíthat
- CEP lehet az ESB része
  - Pl. tartalom alapú továbbítás
- Lehet az egész szolgáltatás CEP alapú…
  - Dinamikus folyamatok
  - Inkább a jövő…

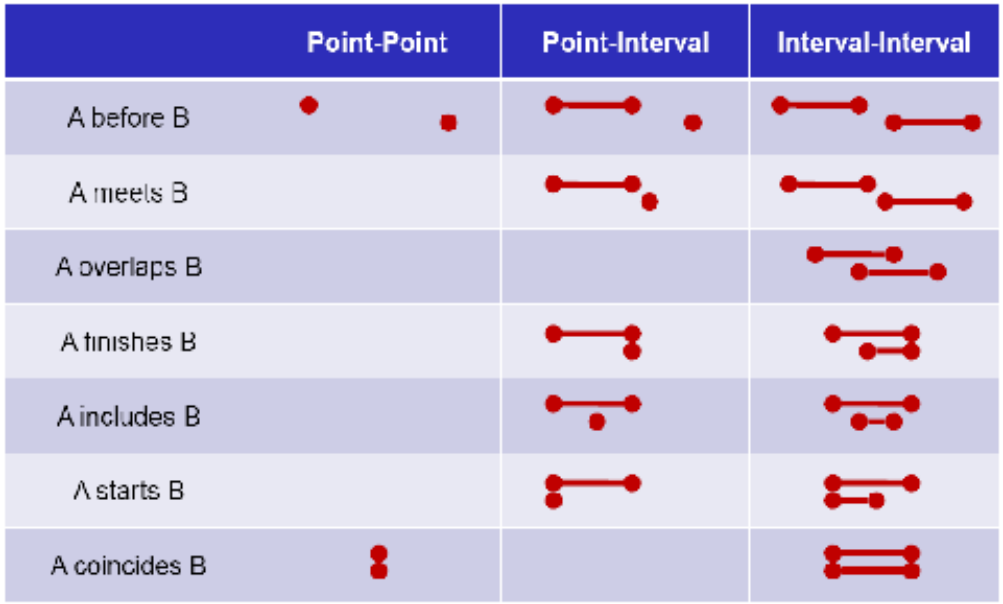
Példa „architektúra”



http://www.packtpub.com/article/cep-complex-event-processing-soa-service-oriented-architecture

Események szemantikája

- Drools:



Alapok:

- Allen-féle intervallum logika, 1983…

```
rule "reasoning on events over time"
when
   $a : A( )
   $b : B( this after[-2,2] $a )
   $c : C( this after[-3,4] $a )
   $d : D( this after[1,2] $b, this after[2,3] $c )
   not E( this after[1,10] $d )
then
   // do something
end
```

CEP eszközök

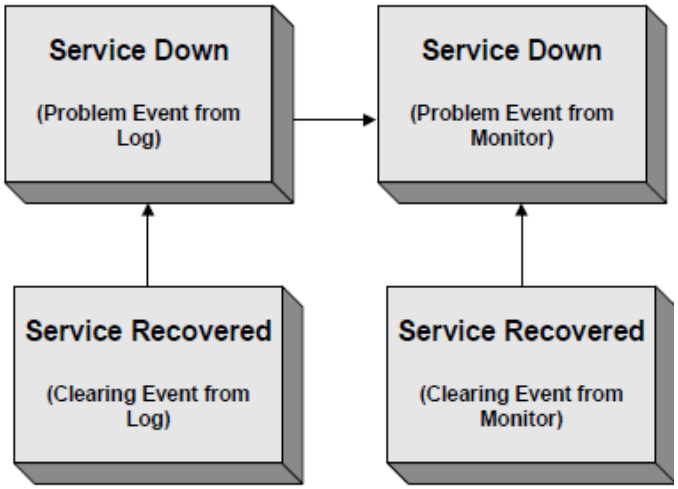
- Számtalan megoldás
  - Esper
  - Drools Fusion
  - IBM InfoSphereStreams (System S), WebSphere Decision Server
  - OpenESB - Intelligent Event Processor
  - Apache Hadoop + ráépülő projektek
  - TIBCO CEP
  - Microsoft StreamInsight
- Döntési szempontok
  - Eseményfeldolgozási logika
  - Áteresztőképesség
  - Elvárt válaszidő („low latency”)

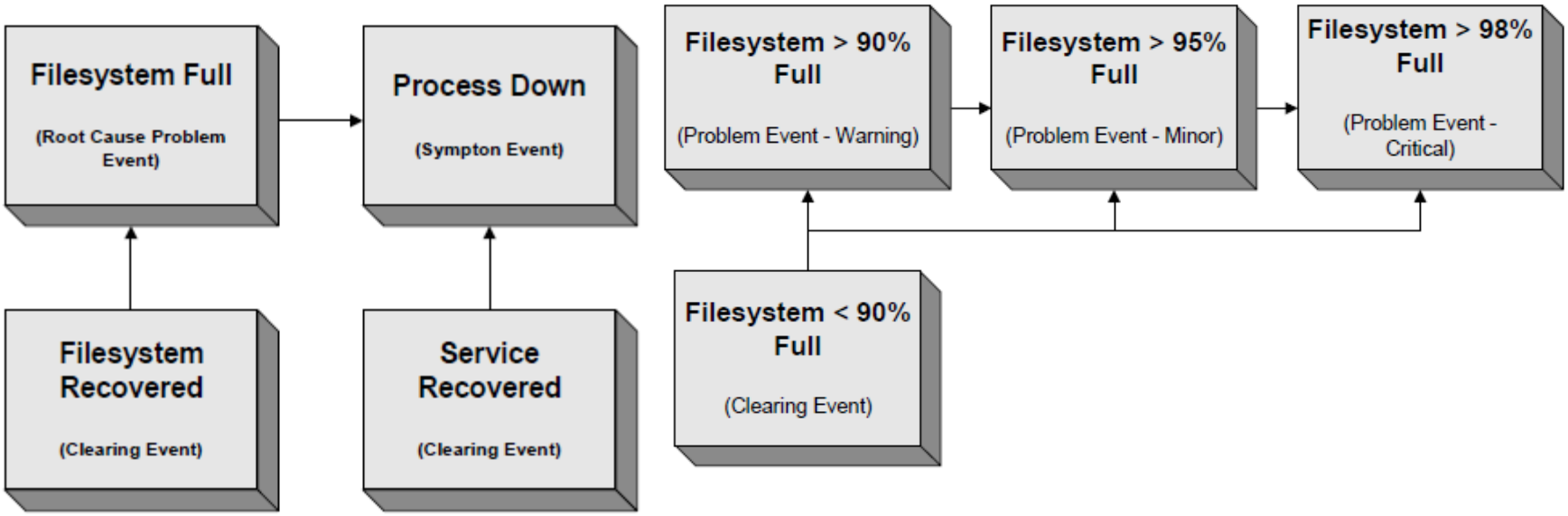
Eseményfeldolgozás lépései

- Előkészítés
  - Események azonosítása („Mi honnan jön?”)
  - Események kiválasztása/szűrése
  - Események kiegészítése
  - Aggregálás
- Elemzés
  - Események „osztályozása” (rating, scoring, classification)
  - Elemzési minták (pl. elnyomás, topológia alapú függőségek figyelembevétele)
  - Események→ komponens állapot
- Feldolgozás
  - Továbbítás
  - Előrejelzés
  - Esemény alapú tanulás

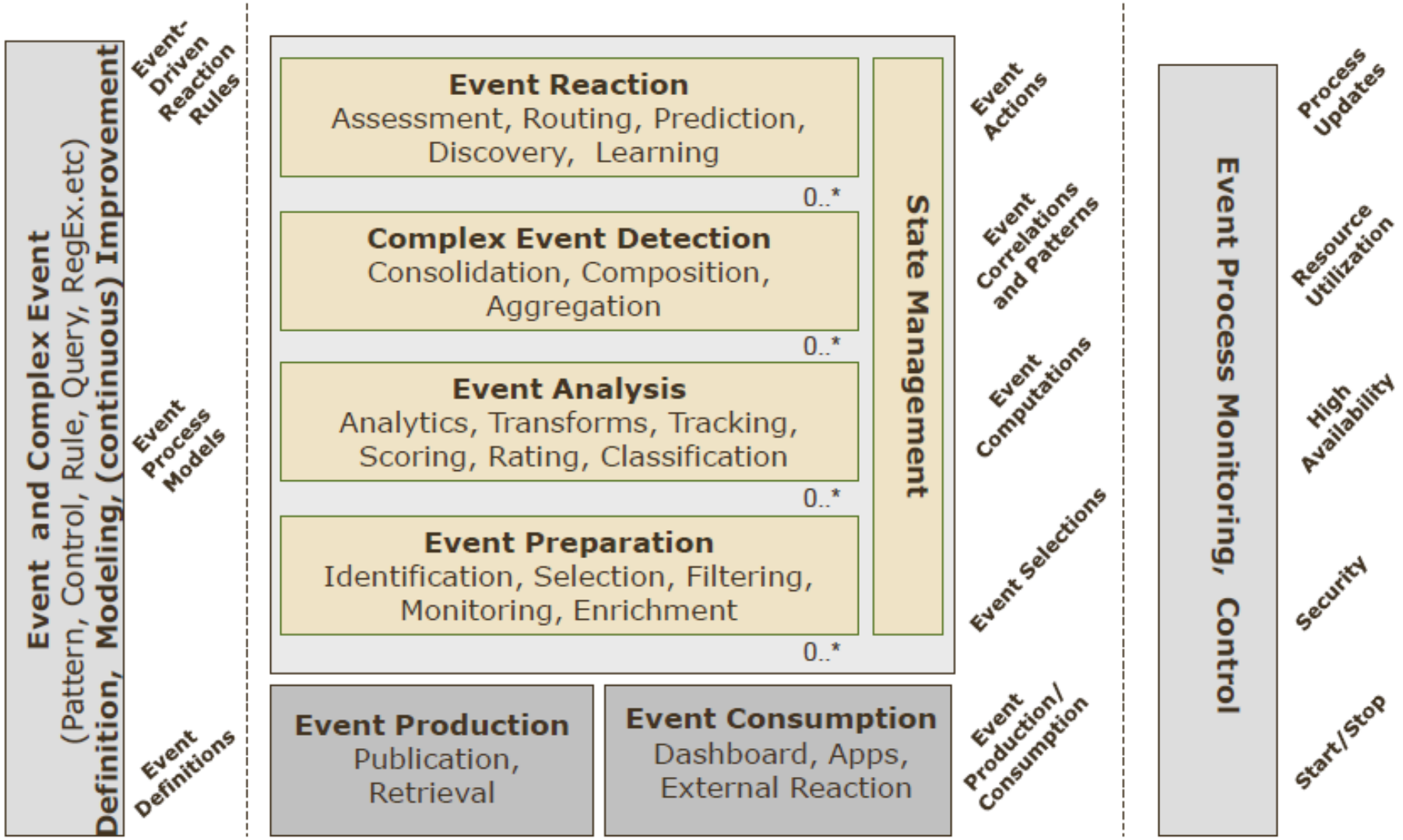
Mit kezdjünk az eseményekkel?

- Korreláció
  - Szolgáltatás leáll- újraindul
- Eszkaláció
- Ok-hatás analízis





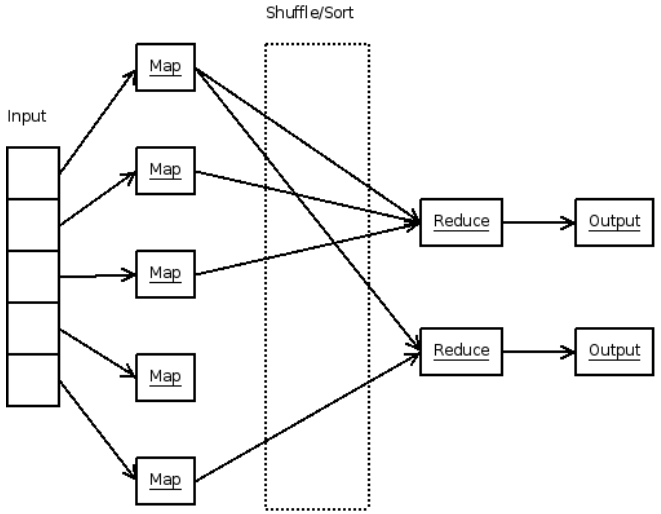
Referencia architektúra/feladatok



Event Processing Technical Group, 2011.

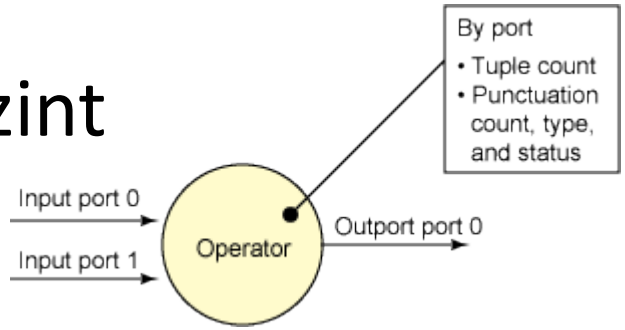
Példa: Map/Reduce algoritmus

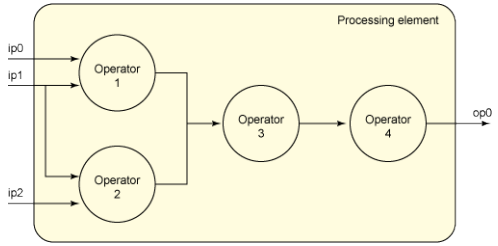
- Map lépés
  - adat felosztása
- Reduce lépés
  - adat feldolgozása
- Példa
  - szöveg felosztása szavakra, szavak számának megállapítása
- Számos programnyelven
- Apache implementáció
  - Elosztott megoldás
  - Hadoop (+ Hadoop Distributed File System)
  - Ütemezés : Job Tracker, Task Tracker



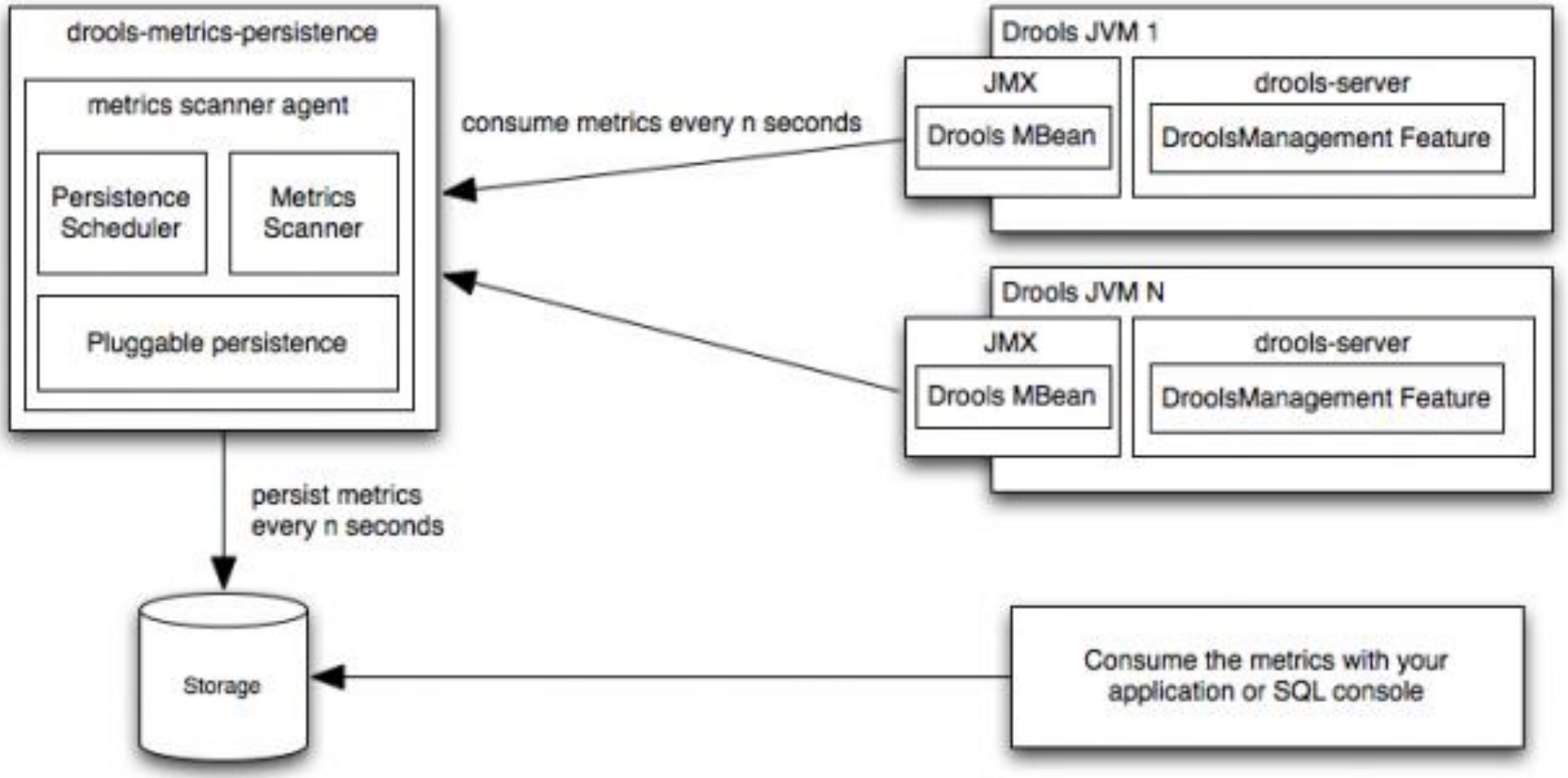
Hogyan mérjük az eseményfeldolgozást?

- Példa: IBM InfoSphere Streams
- Operátor/feldolgozási egység szint
  - Feldolgozott/eldobott adatok
  - Továbbított adatok
  - Sorhossz
- Feldolgozási egység szintje





Példa: Drools metrika gyűjtés

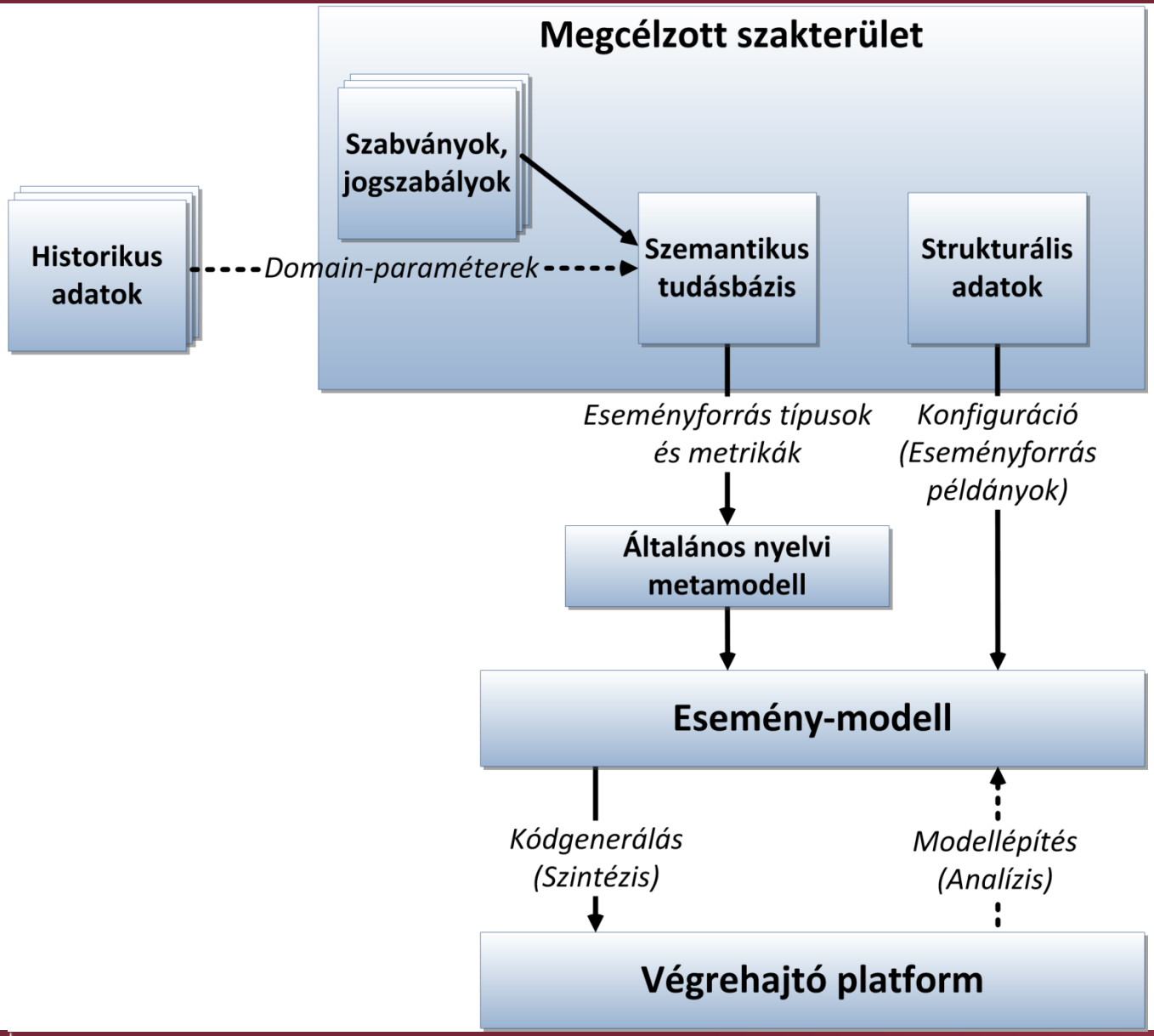


http://lucazamador.wordpress.com/2011/01/07/drools-metrics-persistence/

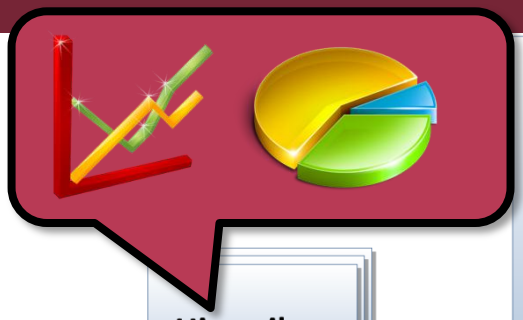
Kihívások

- Események szemantikája
  - Mit jelent? Melyiket figyeljük? (~100 eseményforrás)
  - Milyen kapcsolata van a rendszer dinamikus működésével? (folyamatok)
- Minta alapú tanulás
  - Pl. küszöbértékek hangolása
- Ritka események hatékony azonosítása
- Teljesség? Helyesség?

Példa: modell alapú feldolgozás

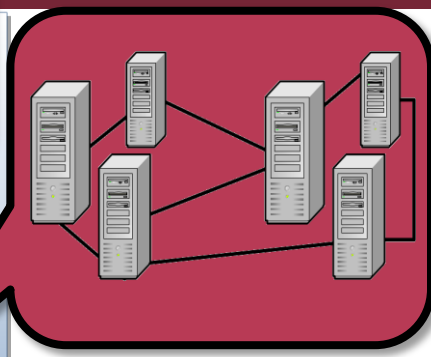


Példa: mode[illegible]ozás



$\mathcal{L}_1$ = { „webszerver”, „szolgáltatás” …}

$\mathcal{L}_2$ = { „kritikus”, „bizalmas” …}



Szabványok, jogszabályok

Historikus adatok

Domain-[illegible]améterek

Szemantikus tudásbázis

Strukturális adatok

Eseményforrás típusok és metrikák

Konfiguráció (Eseményforrás példányok)

COBIT PO6:
Gondoskodni arról, hogy a kritikus és bizalmas információkhoz ne lehessen jogosulatlanul hozzáférni.

Általános nyelvi metamodell

$\mathcal{L}$ = { Event, ComplexEvent, Source …}

Esemény-modell

```
Event WebServerCritical {
  source WebServer1
  LiteralMeasurement
    Authenticated [User]
}
```

A

Kódgenerálás (Szintézis)

Modellépítés (Analízis)

```
select fraud.
accountNumber as
aNm,fraud.warning
as warn
from
FraudEvent.win:
time(30 min) as fd
…
```

Végrehajtó platform

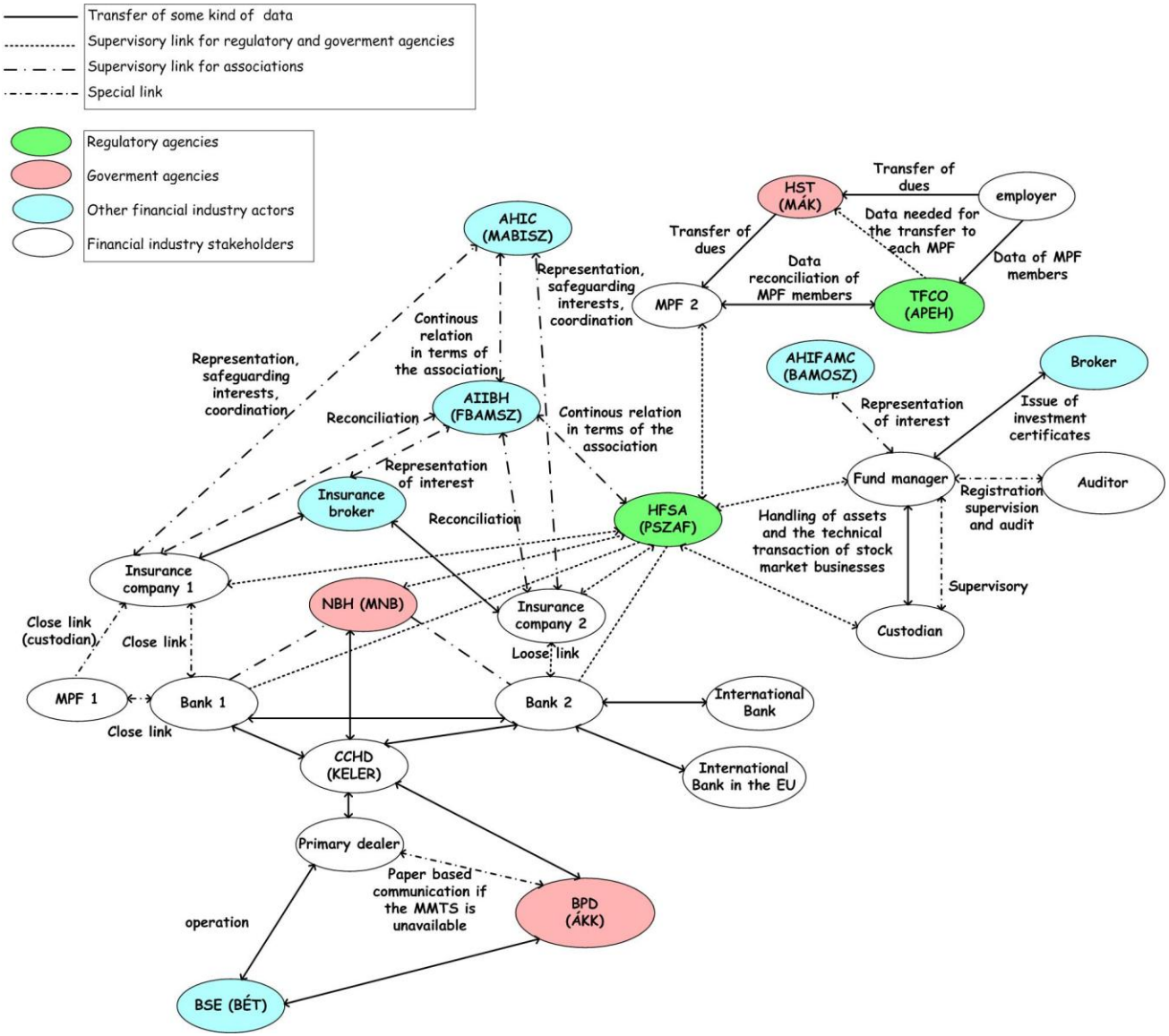
Esettanulmány: CoMiFin

Szolgáltatásalapú rendszerek, modellvezérelt fejlesztés, komplex eseményfeldolgozás,…

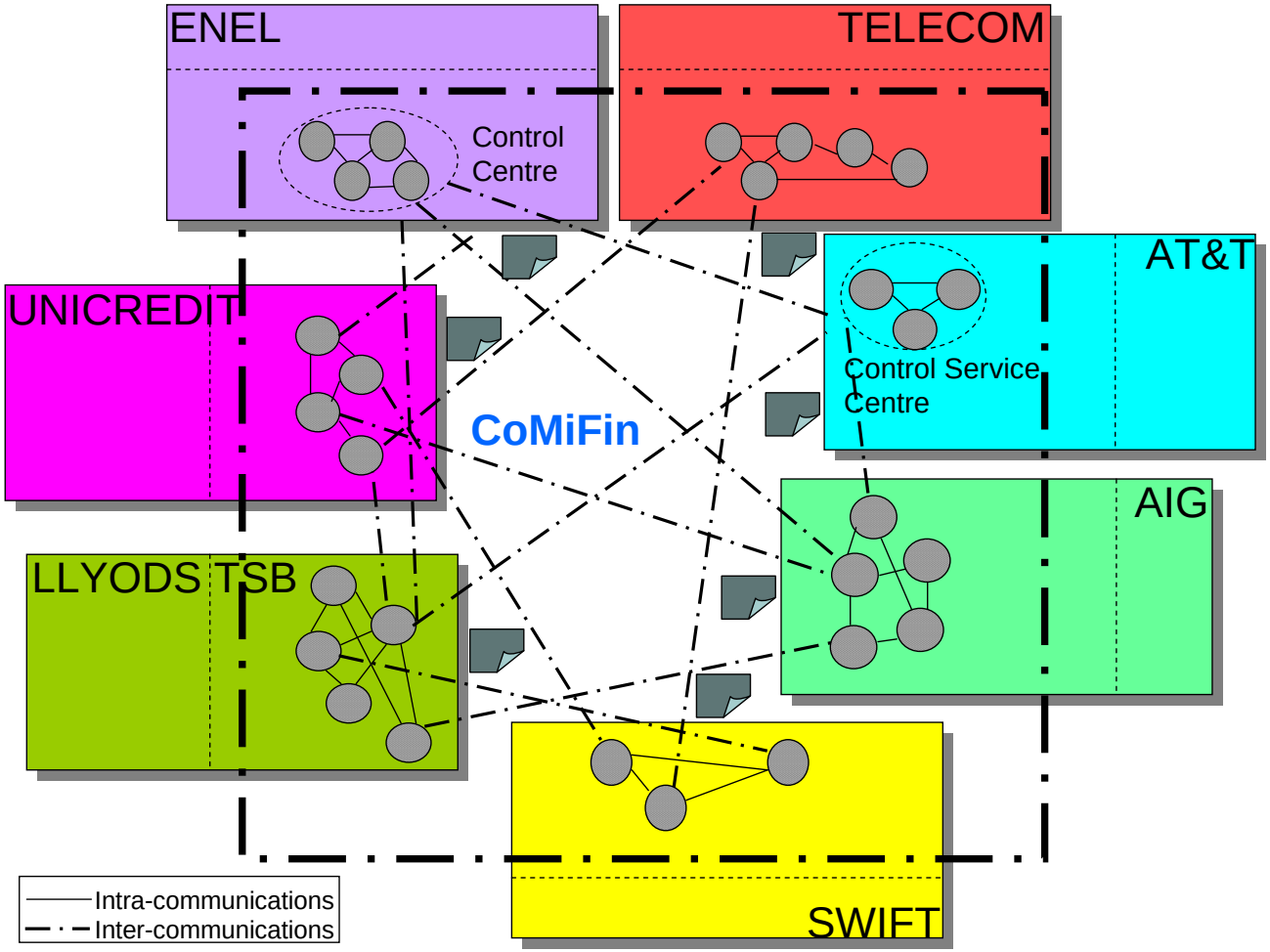
Esettanulmány: CoMiFin

- „Communication Middleware for Financial Infrastructures”
- Motiváció
  - Banki rendszerek egyre erősebben függenek külső szolgáltatóktól
  - Támadások egyre kifinomultabbak
  - Kritikus infrastruktúrák (pl. mobilhálózat, áramellátás, Internet) elleni komplex támadások kivédése
  - Hagyományos kommunikáció lassú (példa: 8 nap egy eset lezárása)
- Cél
  - Scheme to set up and manage a secure environment (software, hardware, monitoring tools, etc.) for information exchange and analysis
- Tanszéki spin-off (OptXware) vezette a demonstrátor fejlesztését

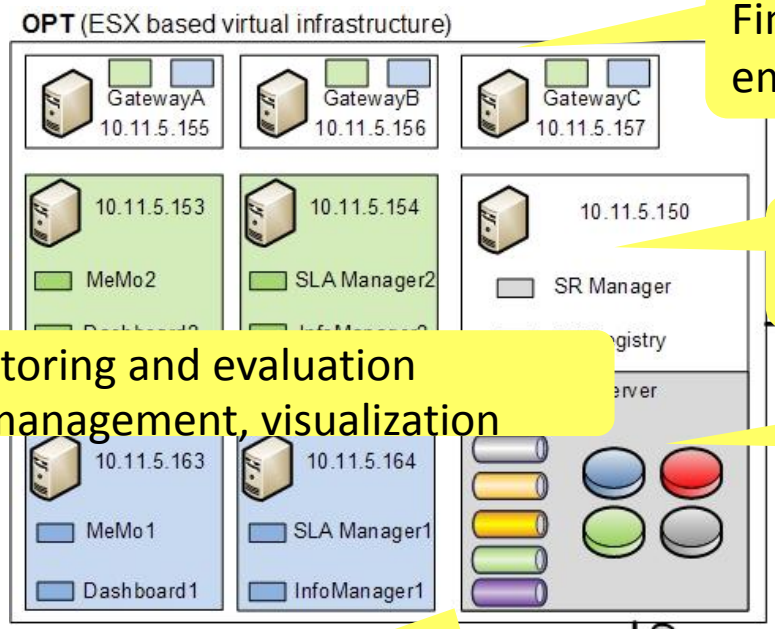
Példa: magyar infrastruktúra

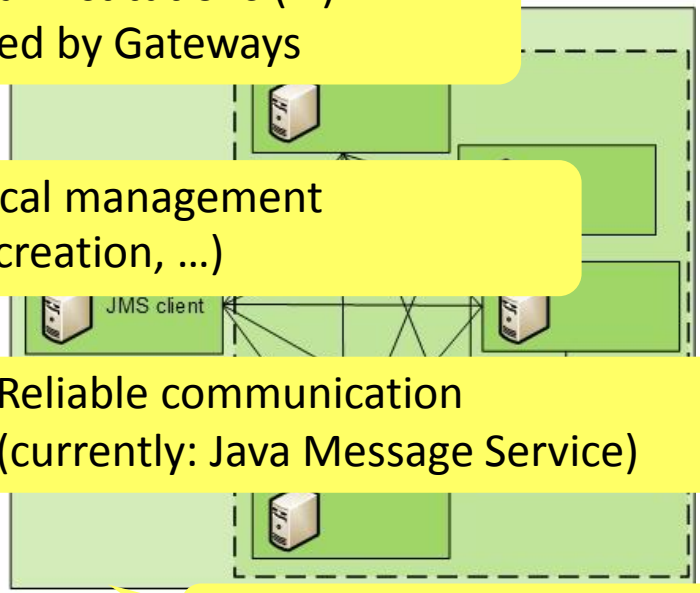


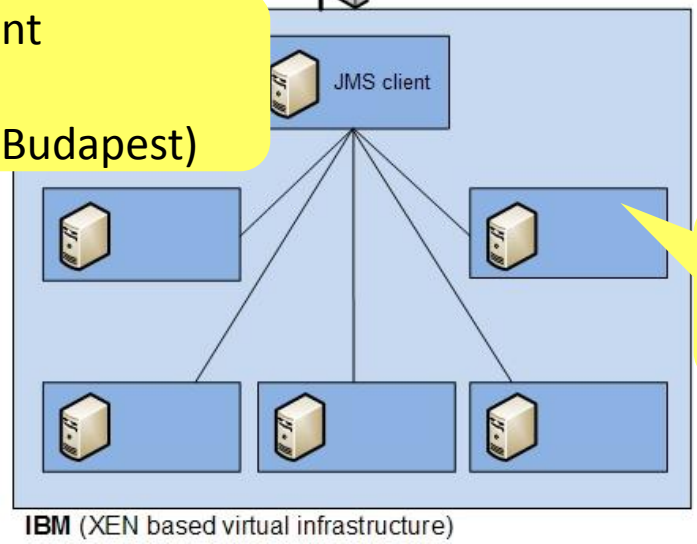
Logikai architektúra



Architektúra







Financial Institutions (FI)
emulated by Gateways

Logical management
(SR creation, …)

Monitoring and evaluation
SLA management, visualization

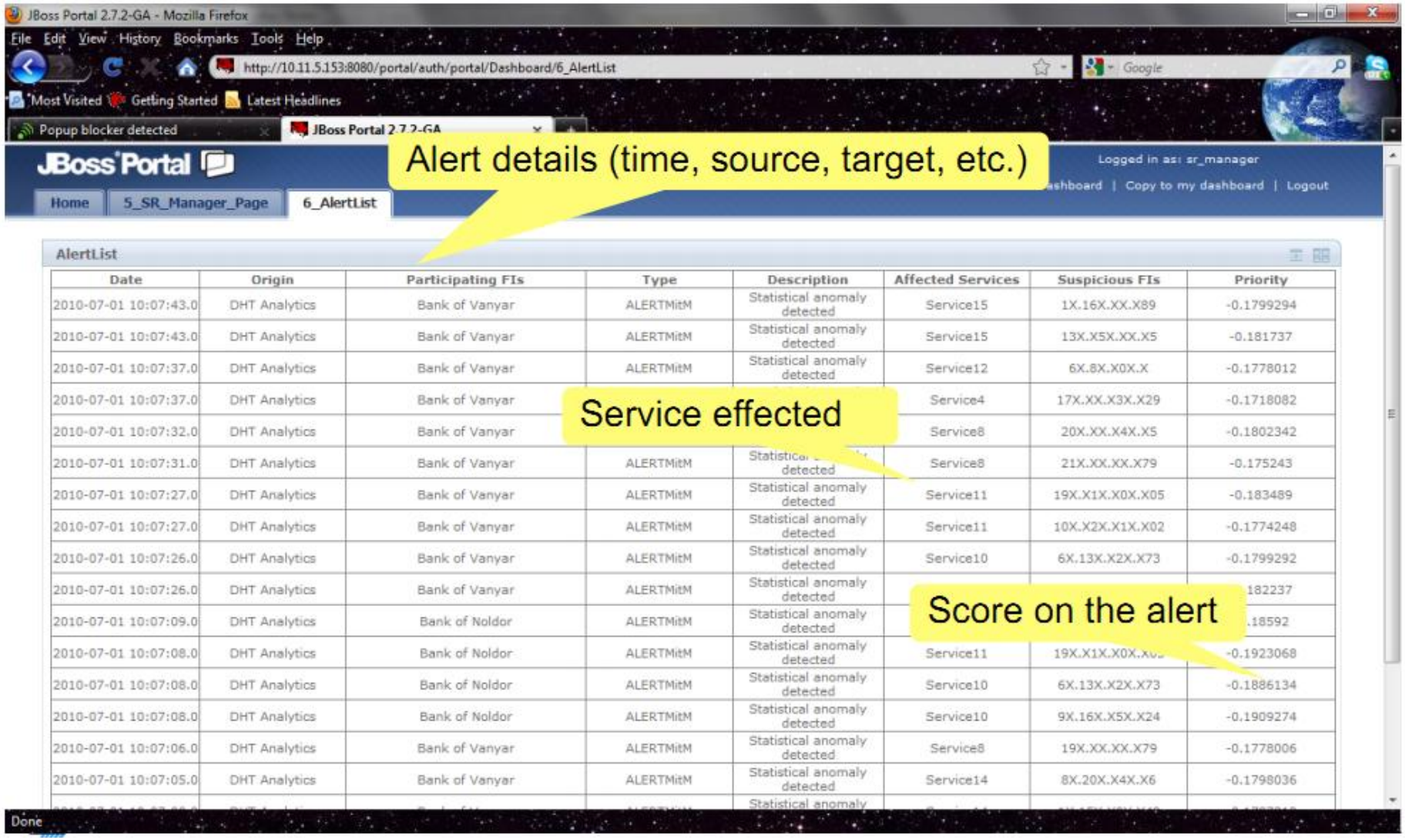
Reliable communication
(currently: Java Message Service)

ED Event Processing (DHT)
(ED Testbed, Rome)

CoMiFin management
components
(OptXware testbed, Budapest)

IBM Event Processing
(AGILIS)
(IBM Testbed, Haifa)

Eredmények megjelenítése



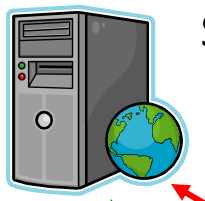
AlertList

Date	Origin	Participating FIs	Type	Description	Affected Services	Suspicious FIs	Priority
2010-07-01 10:07:43.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service15	1X.16X.XX.X89	-0.1799294
2010-07-01 10:07:43.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service15	13X.X5X.XX.X5	-0.181737
2010-07-01 10:07:37.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service12	6X.8X.X0X.X	-0.1778012
2010-07-01 10:07:37.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service4	17X.XX.X3X.X29	-0.1718082
2010-07-01 10:07:32.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service8	20X.XX.X4X.X5	-0.1802342
2010-07-01 10:07:31.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service8	21X.XX.XX.X79	-0.175243
2010-07-01 10:07:27.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service11	19X.X1X.X0X.X05	-0.183489
2010-07-01 10:07:27.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service11	10X.X2X.X1X.X02	-0.1774248
2010-07-01 10:07:26.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service10	6X.13X.X2X.X73	-0.1799292
2010-07-01 10:07:26.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected			182237
2010-07-01 10:07:09.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected			.18592
2010-07-01 10:07:08.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service11	19X.X1X.X0X.X	-0.1923068
2010-07-01 10:07:08.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service10	6X.13X.X2X.X73	-0.1886134
2010-07-01 10:07:08.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service10	9X.16X.X5X.X24	-0.1909274
2010-07-01 10:07:06.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service8	19X.XX.XX.X79	-0.1778006
2010-07-01 10:07:05.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service14	8X.20X.X4X.X6	-0.1798036

Session Hijack detektálás

- Session hijack: felhasználó forgalmának figyelésével beleavatkozni a munkamenetbe
- Környezet: egyszerű e-Banking alkalmazás
  - Felhasználók kezelése
  - Tranzakciók indítása
- Alkalmazás specifikus információ monitorozása
  - Kliens IP címe
  - Session azonosító
- „Hibainjektálás”

Session Hijacking



Application Server

Ordinary Client

Bad Guy

Main Page

Welcome Ordinary Client!

Your IP address at login time was: 127.0.0.1, your current IP is: 10.11.1.248

Your session ID is: 82B02592FCD04883F13B1C29272642AA

You can choose one of the following actions

Transfer Money

Your previous transfer of 2000 to 12345 has been accepted.

Amount:

IBAN:

Transfer | Empty fields

Logout

Please click to logout.

http://localhost:8080/TestWebApp/HelloServlet;jsessi

Welcome Ordinary Client!

Your IP address at login time was: 127.0.0.1, your current IP is: 127.0.0.1

Your session ID is: 82B02592FCD04883F13B1C29272642AA

You can choose one of the following actions

Transfer Money

Amount:

IBAN:

Transfer | Empty fields

Logout

Please click to logout.

Main Page

Welcome Bad Guy!

Your IP address at login time was: 10.11.1.248, your current IP is: 10.11.1.248

Your session ID is: A3ED6B154F6F303B808B056AF6923CBC

You can choose one of the following actions

Transfer Money

Amount:

IBAN:

Transfer | Empty fields

Logout

Please click to logout.

Session hijack detektálás

- Az IP és a session ID Drools alapú ellenőrzésével

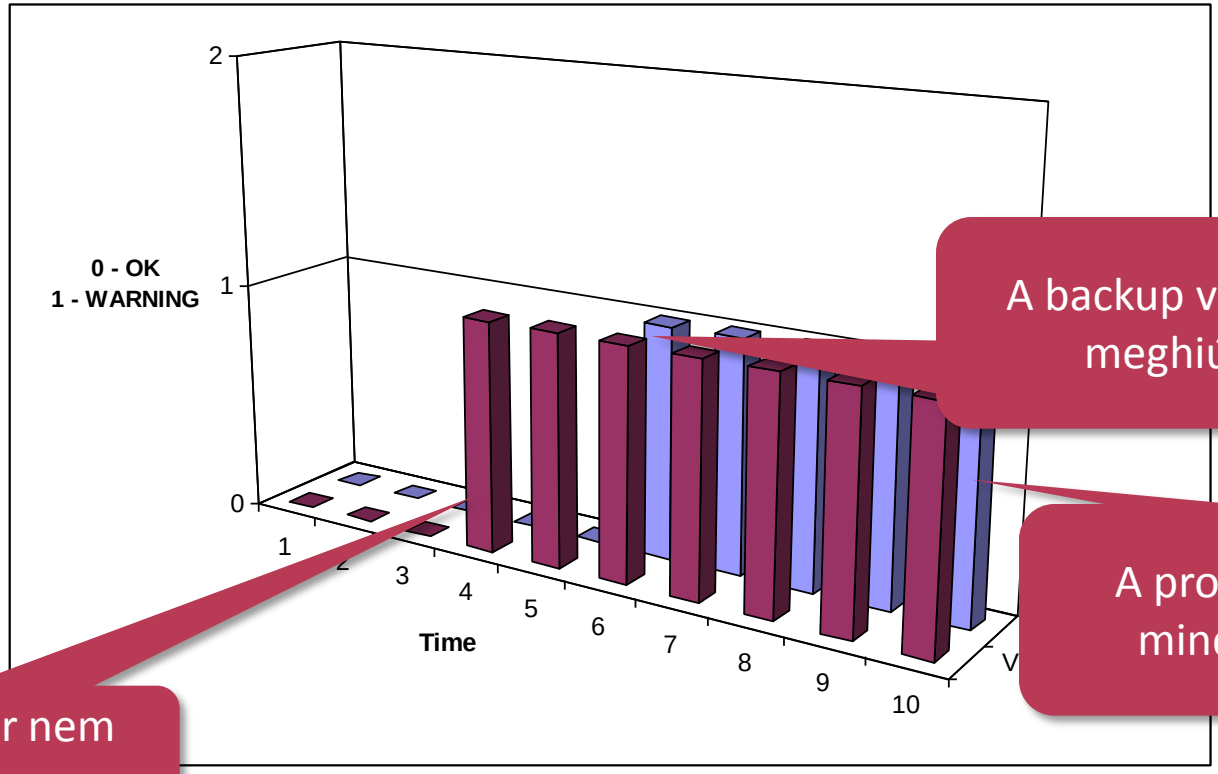
```
WARNING: possible session hijack:
{
 currentAddress=127.0.0.1,
 remoteAddress=127.0.0.1,
 sessionId=21...B6
}
and the possible attacker with the same session:
{
 currentAddress=10.11.1.154,
 remoteAddress=127.0.0.1,
 sessionId=21...B6
}
```

Demonstrations

- Demo 2: Késedelmes backup felderítése
  - Több alkalmazásból érkező információ
  - Komplex esemény
  - Vonatkozó előírások:
    - e.g. COBIT PO-4 “Define the IT Processes, Organization and Relationships”
    - COBIT PO-9 “Manage IT Human Resources”

Késedelmes mentés detektálása

- Monitorozott szolgáltatások
  - Backup (storage alrendszer, adatbázis, stb.)
  - Az adminisztrátor bejelentkezése
- Időzítés szimulációs alapon



A backup valamiért meghiúsult

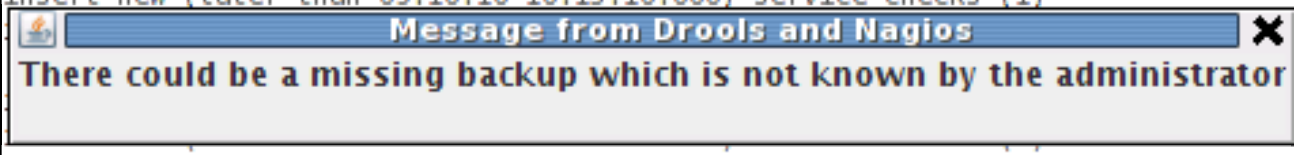
A probléma még mindig fennáll

Adminisztrátor nem aktív

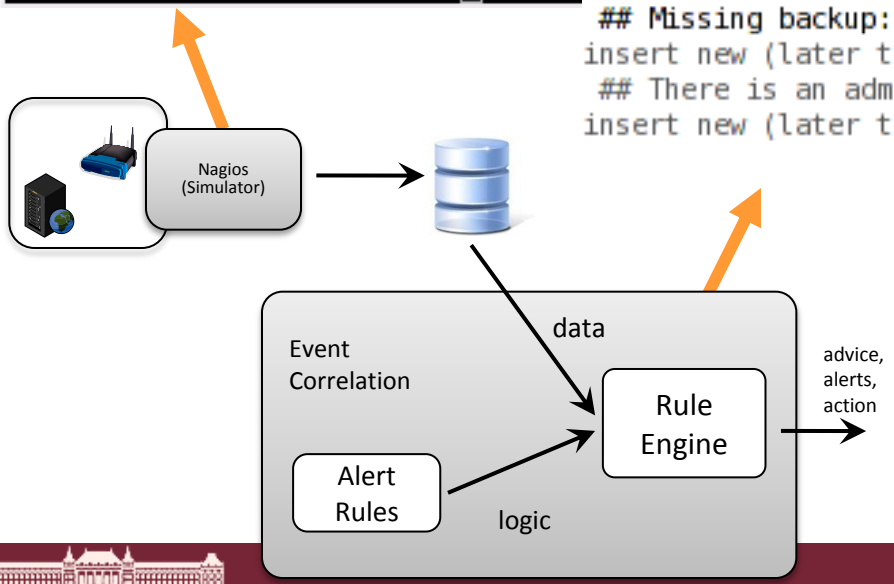
Drools alapú detektálás

```
[root@p2 NagiosDrools5]# sh runSimulator.sh "2009-10-10 10:10:10" 0.01
Press enter to start simulation

Press enter to stop simulation
Next sleep time is 1800
Next sleep time is 1200
Next sleep time is 1800
Next sleep time is 1200
Next sleep time is 1800
Next sleep time is 1200
Next sleep time is 1800
Next sleep time is 1200
Next sleep time is 1800
Next sleep time is 1200
Next sleep time is 1800
Next sleep time is 3000
Insertion of events finished

[root@p2 NagiosDrools5]#
```

```
INFO: Feeder has been started
Press enter to exit
insert new (later than 09.10.10 10:10:10.000) service checks (1)
insert new (later than 09.10.10 10:13:10.000) service checks (1)
 ## There is an administrator missing ServiceCheck(3): 10:15:10.000 (1)
insert new (later than 09.10.10 10:15:10.000) service checks (1)
```




```
 ## There is an administrator missing ServiceCheck(7): 10:25:10.000 (1)
insert new (later than 09.10.10 10:25:10.000) service checks (1)
 ## There could be a missing backup which is not known by the administrator
 ## Missing backup: ServiceCheck(8): 10:28:10.000 (1)
insert new (later than 09.10.10 10:28:10.000) service checks (1)
 ## There is an administrator missing ServiceCheck(9): 10:30:10.000 (1)
insert new (later than 09.10.10 10:30:10.000) service checks (1)
```



Esettanulmány: IT infrastruktúra események monitorozása

Dávid István, Gönczy László

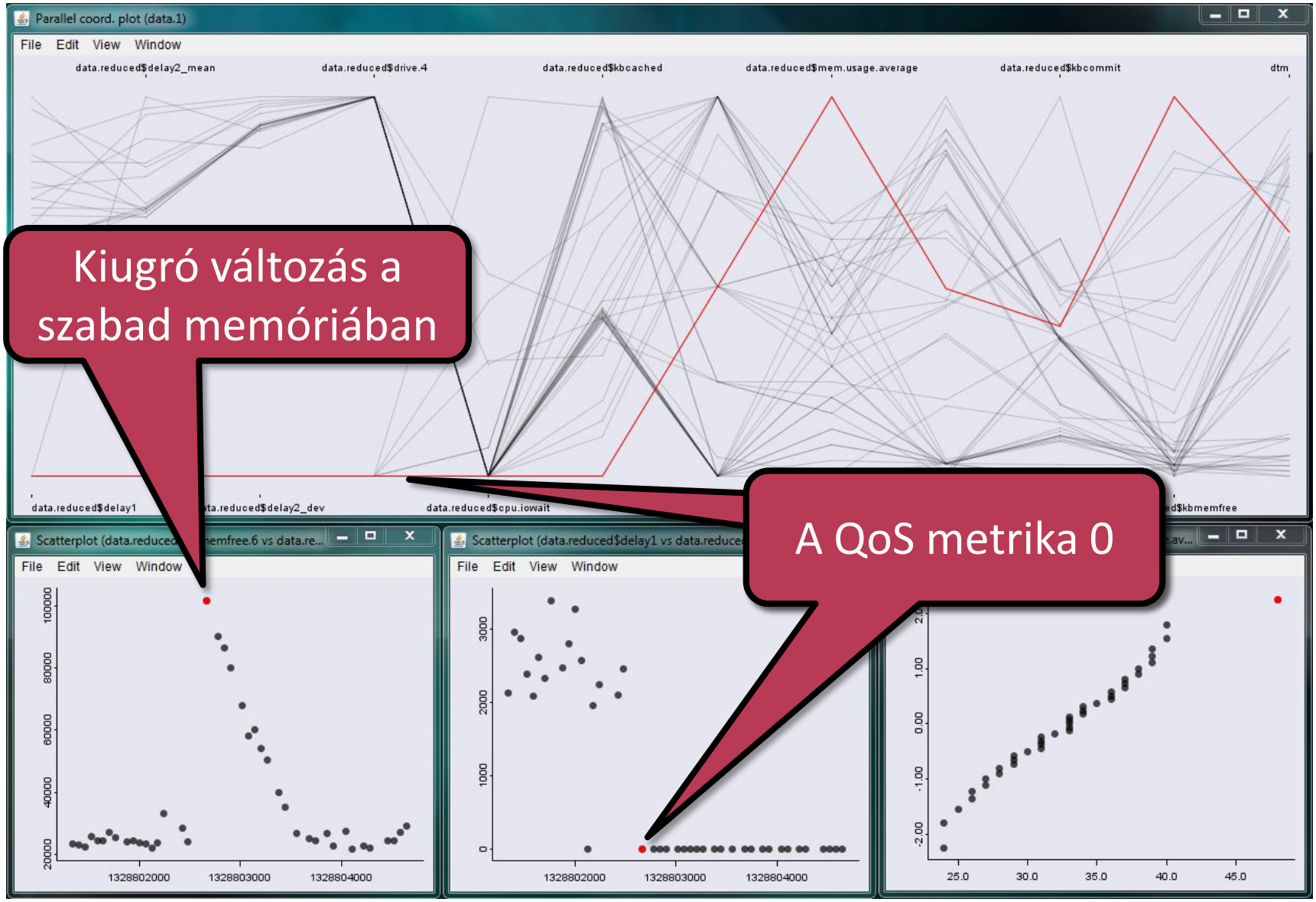
Modellalapú fejlesztési módszer komplex események feldolgozásához (European Dependable Computing Conference2012, Mesterpróba 2012)

Esettanulmány

- BigBlueButton
- Többféle mért attribútum
  - CPU terheltség, rendelkezésre álló memória, cache…
  - QoS metrikák: az audiovizuális adat késleltetése
- A rendszer túlterheltségének karakterisztikája:
  - A mért késleltetés 0 (definíció szerint)
  - Hirtelen növekedés a szabad memóriában
  - Fail-silent működés
- A cél:
  - Detektáljuk a túlterhelést és konfiguráljuk újra a rendszert
- Az **eseményfolyam** ebben az esetben: Az infrastruktúra elemek metrikáinak folyamatosan mért értékei

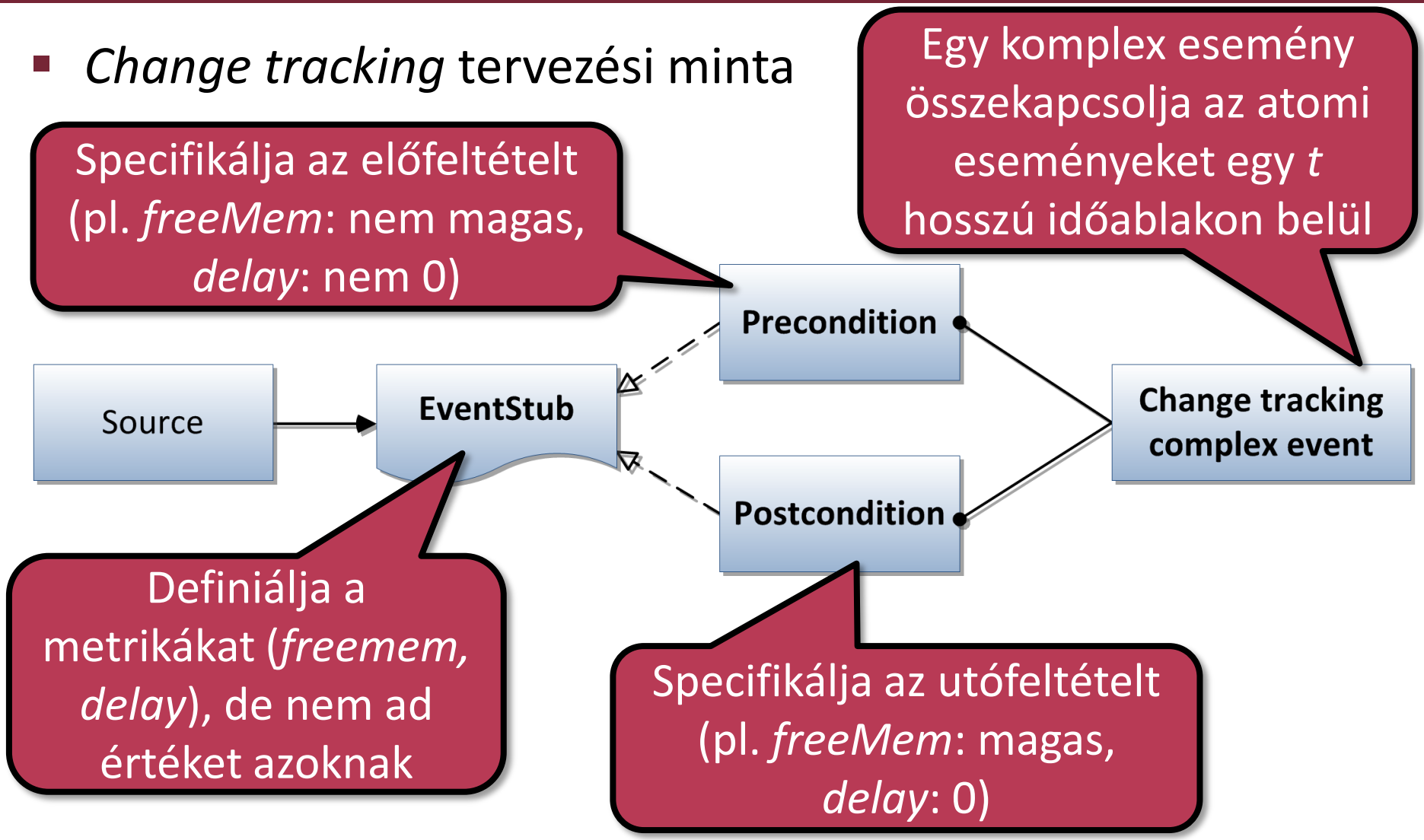
Imre Kocsis, András Pataricza, Zoltán Micskei, István Szombath, András Kövi & Zsolt Kocsis Cloud Based Analytics for Cloud Based Applications, ICA CON 2012.

Túlterhelés vizuálisan ábrázolva



A modellezés áttekintése

- *Change tracking* tervezési minta



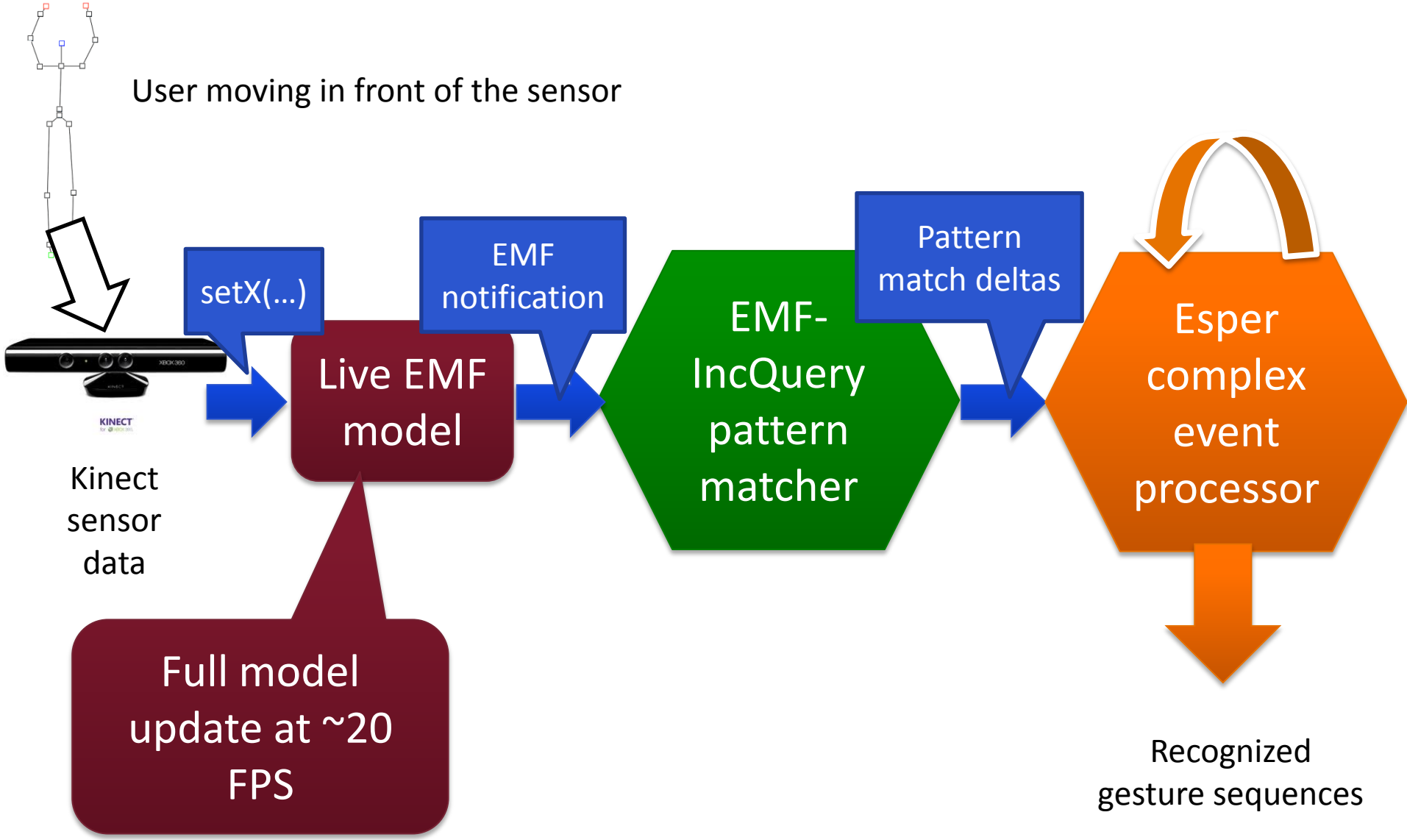
Esettanulmány: valósidejű gesztusfelismerés

"Standing Queries"
Realtime gesture recognition with Eclipse technologies

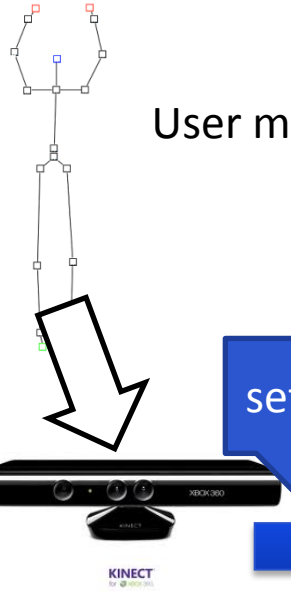
Dávid István, Ráth István

EclipseCon Europe 2012

Overview


User moving in front of the sensor
setX(...)
EMF notification
Pattern match deltas
Live EMF model
EMF-IncQuery pattern matcher
Esper complex event processor
Kinect sensor data
Full model update at ~20 FPS
Recognized gesture sequences

Overview



User moving in front of tl

setX(...)

not

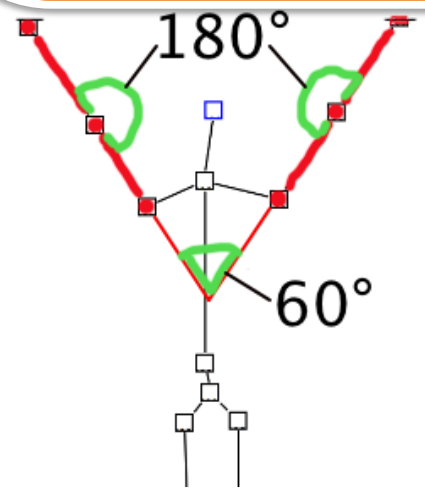
Live EMF model

Kinect sensor data

Full model update at ~20 FPS

Event Pattern YMCA

```
SELECT * FROM pattern[
 every(('Y') ->
              ('M') ->
              ('C') ->
              ('A')
WHERE timer:within(10 sec))]
```

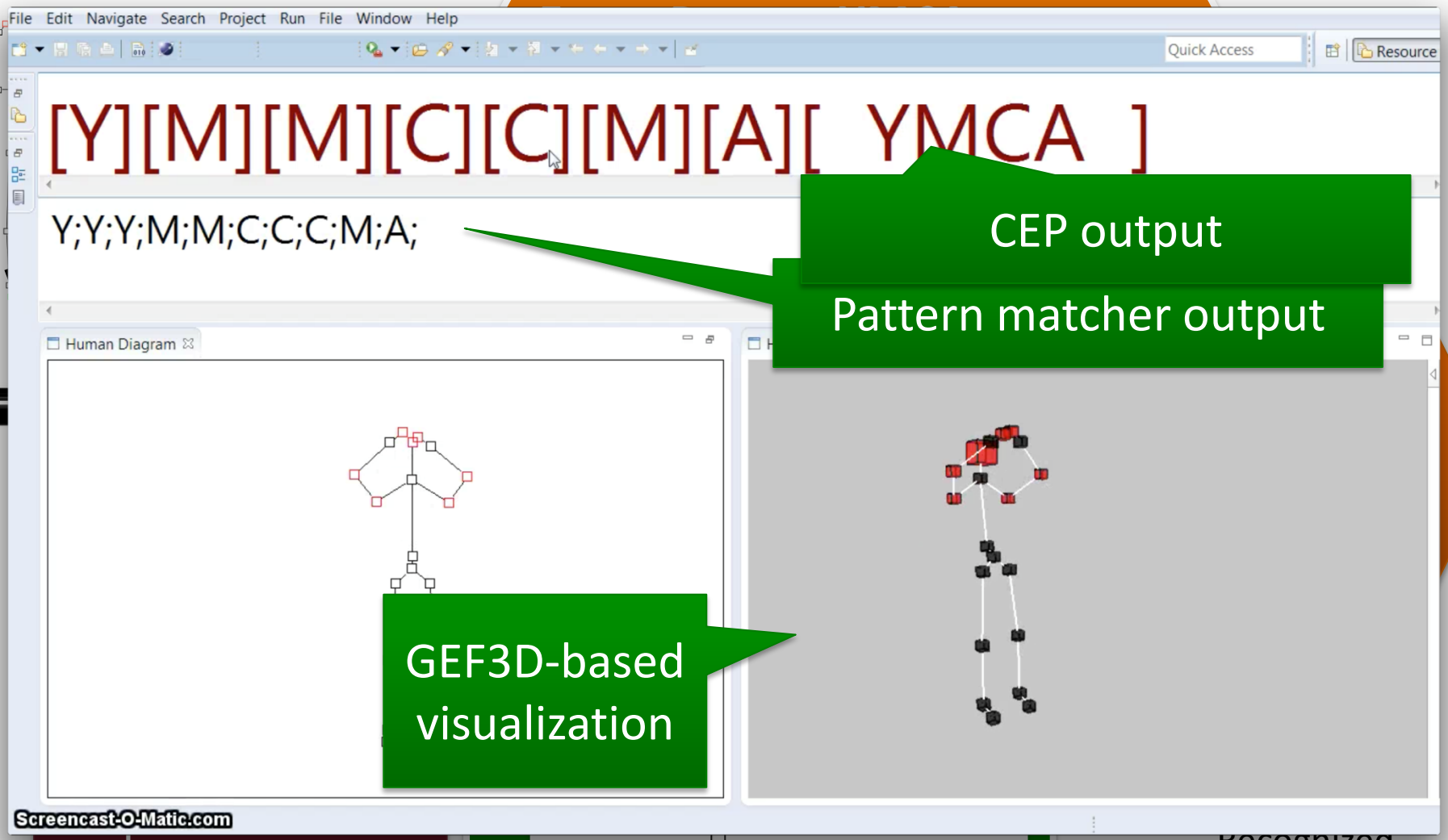


}

sper
lex
event
processor

Recognized gesture sequences

Overview



FPS

Recognized gesture sequences

Források

- http://www.complexevents.com/
- http://www.slideshare.net/isvana/epts-debs2011-event-processing-reference-architecture-and-patterns-tutorial-v1-2
- http://www.ibm.com/developerworks/data/library/techarticle/dm-1203infostreamsfeatures1/index.html
- http://www.jboss.org/drools/drools-fusion.html
- http://www.thetibcoblog.com/2010/03/04/how-does-cep-fit-into-bpm-and-soa-environments/
- http://tdk.aut.bme.hu/Conf/TDK2011/szoftver/Modellalapu-fejlesztesi
- http://www.packtpub.com/article/cep-complex-event-processing-soa-service-oriented-architecture
- http://books.google.hu/books?id=tx2NXQEo47EC&printsec=frontcover&hl=hu#v=onepage&q&f=false
- http://bpt.hpi.uni-potsdam.de/pub/Public/GeroDecker/edoc2007-eventlanguage.pdf
- http://www.soa.si/wp-content/documents/clanki/WSDL_and_BPEL_extensions_for_Event_Driven_Architecture.pdf
- http://public.dhe.ibm.com/software/data/sw-library/infosphere/casestudy/Assessing-Transport-Systems-casestudy-in-Dublin.pdf
- http://www.slideshare.net/opher.etzion/debs2009-event-processing-languages-tutorial