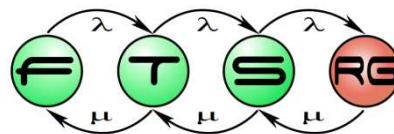


Komplex eseményfeldolgozás (CEP)

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 servermetrika, százas nagyságrendű server
- 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
- Elosztott adatforrások
 - Adatbázisok, beérkező kérések, megfigyelt események, stb.
- Skálázhatóság
 - Cloud környezet

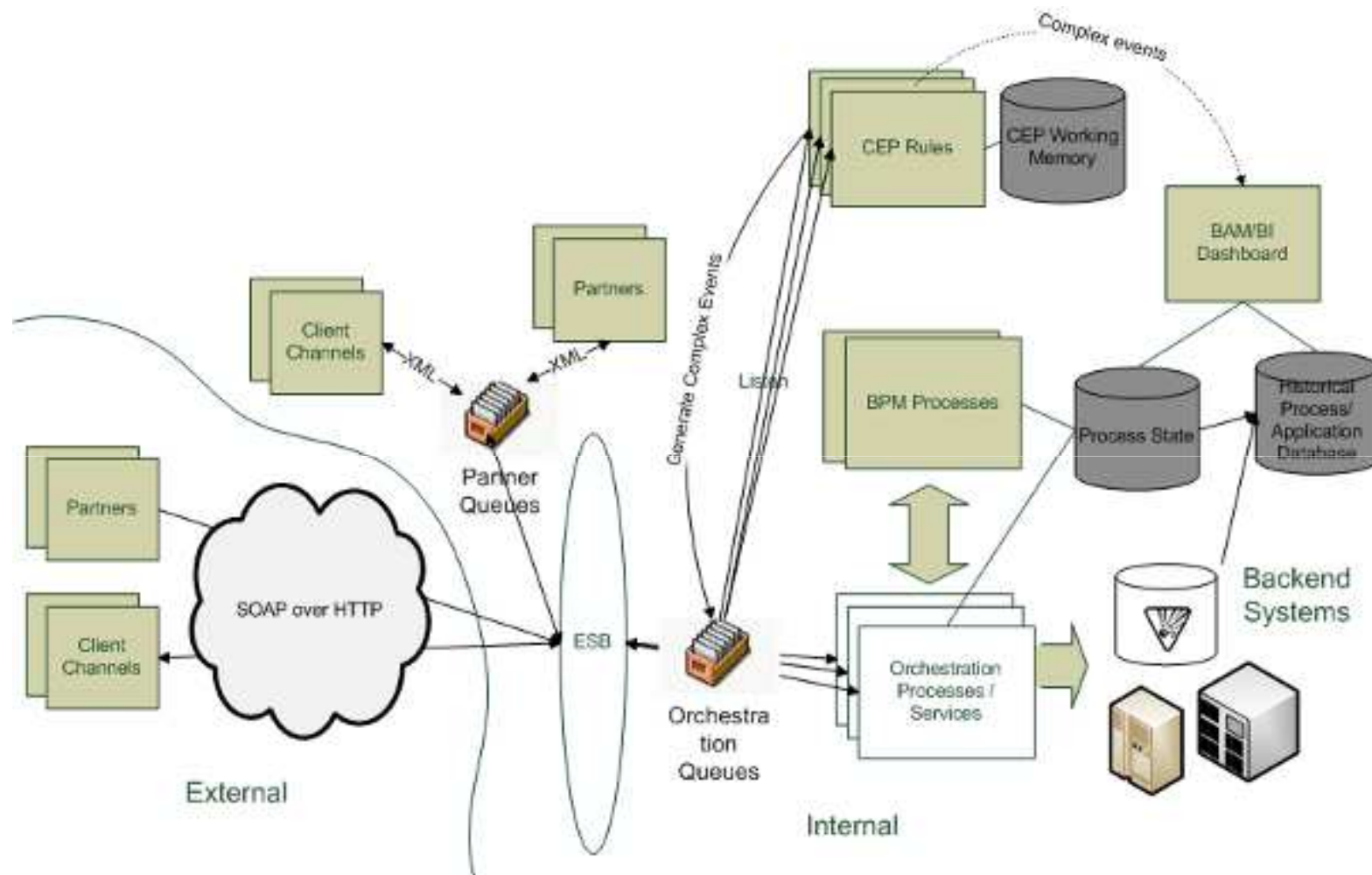
CEP alkalmazási területek

- Üzleti alkalmazások
 - Tőzsde, befektetések
 - „Treasury”
 - Kockázatkértékelés
 - 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 Szolglnt

- 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:

	Point-Point	Point-Interval	Interval-Interval
A before B			
A meets B			
A overlaps B			
A finishes B			
A includes B			
A starts B			
A coincides B			

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

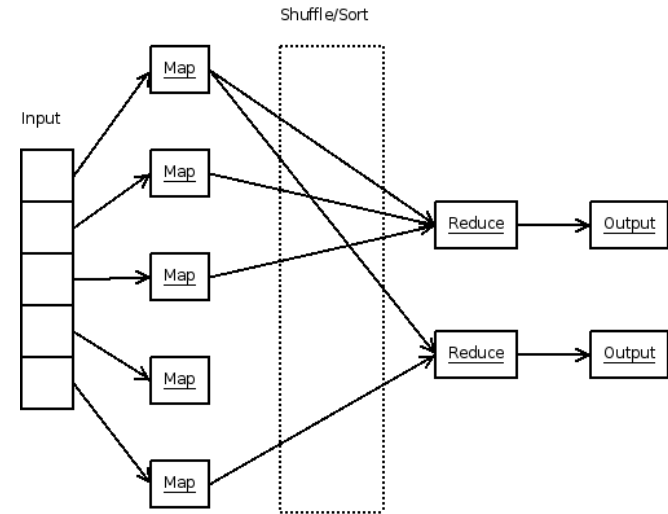
- Számptalan megoldás
 - Esper
 - Drools Fusion
 - IBM InfoSphereStreams (System S), WebSphere Decision Server
 - OpenESB - Intelligent Event Processor
 - Apache Hadoop + ráépülő projektek
 - TIBCO CEP
 - Microsoft StreamInsight
- Döntési szempontok
 - Eseményfeldolgozási logika
 - Áteresztőképesség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

Eseményfeldolgozás lépései

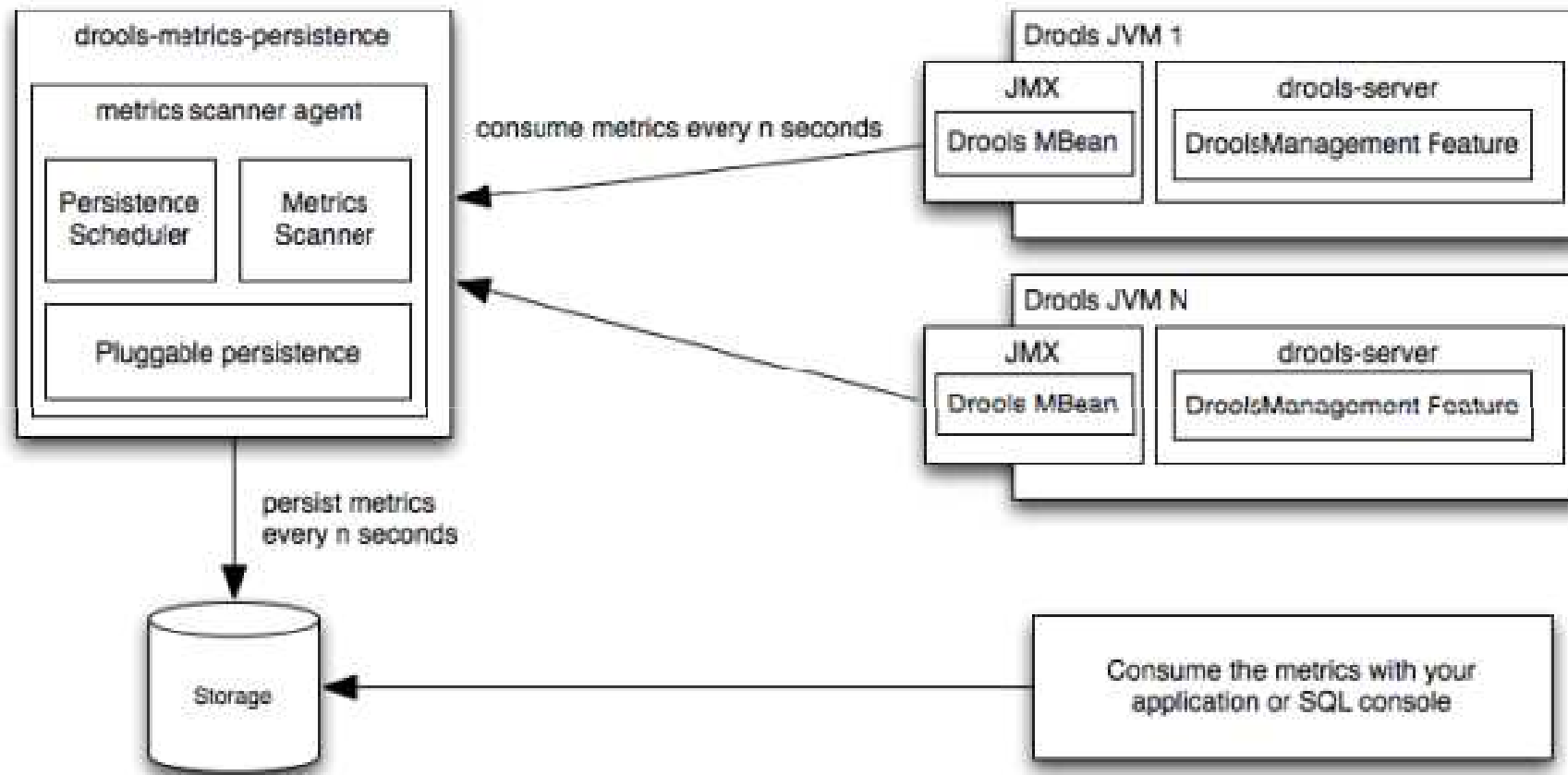
- Előkészítés
 - Események azonosítása („Mi honnan jön?”)
 - Események kiválasztása/szűrése
 - Események kiegészítése
 - Aggregálás
- Elemzés
 - Események „osztályozása” (rating, scoring, classification)
 - Elemzési minták (pl. elnyomás, topológia alapú függőségek figyelembevétele)
 - Események → komponens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

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



Példa: Drools metrika gyűjtés



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

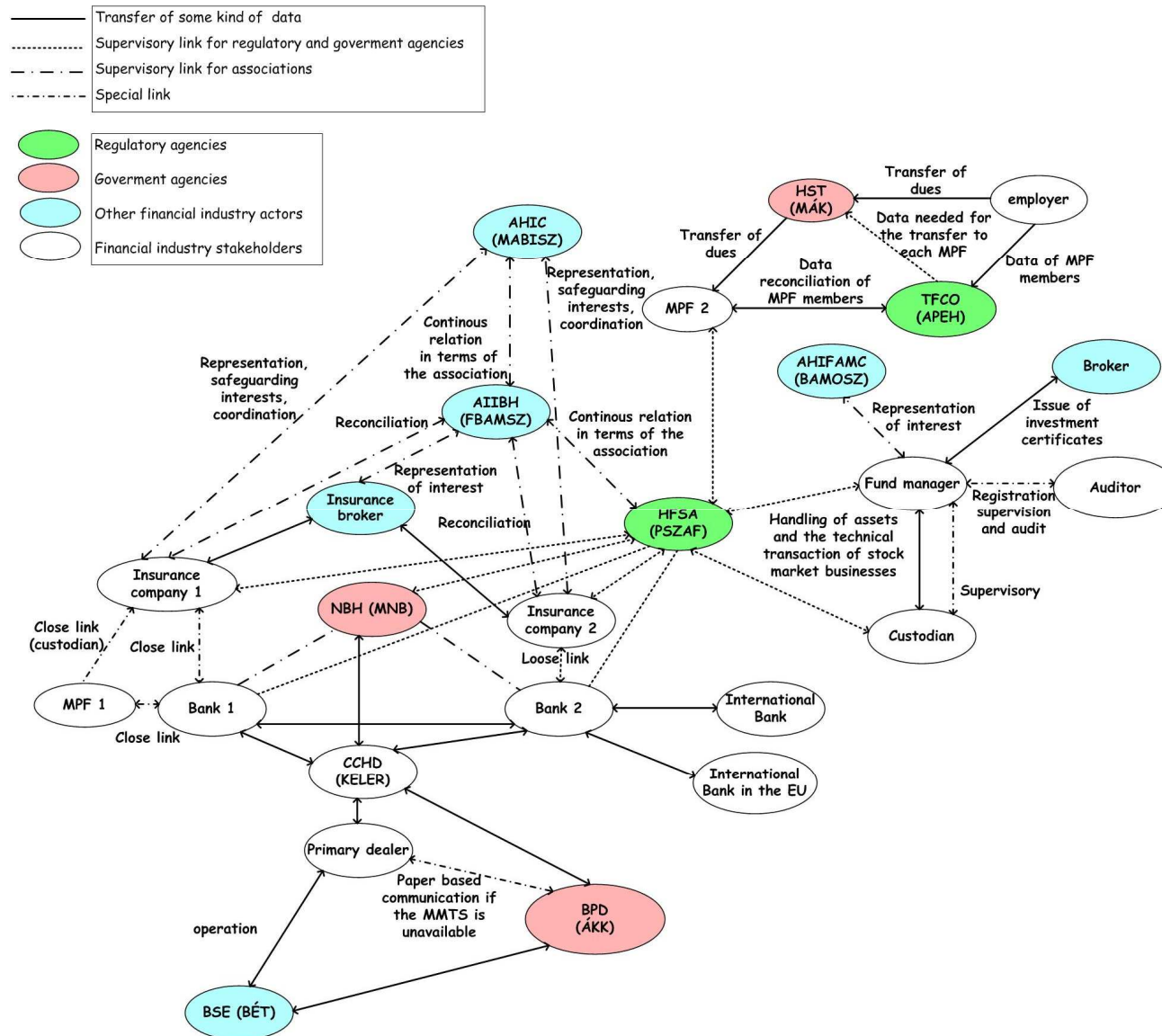
Esettanulmány: CoMiFin

Szolgáltatásalapú rendszerek, modellvezérelt fejlesztés,
komplex eseményfeldolgozás,...

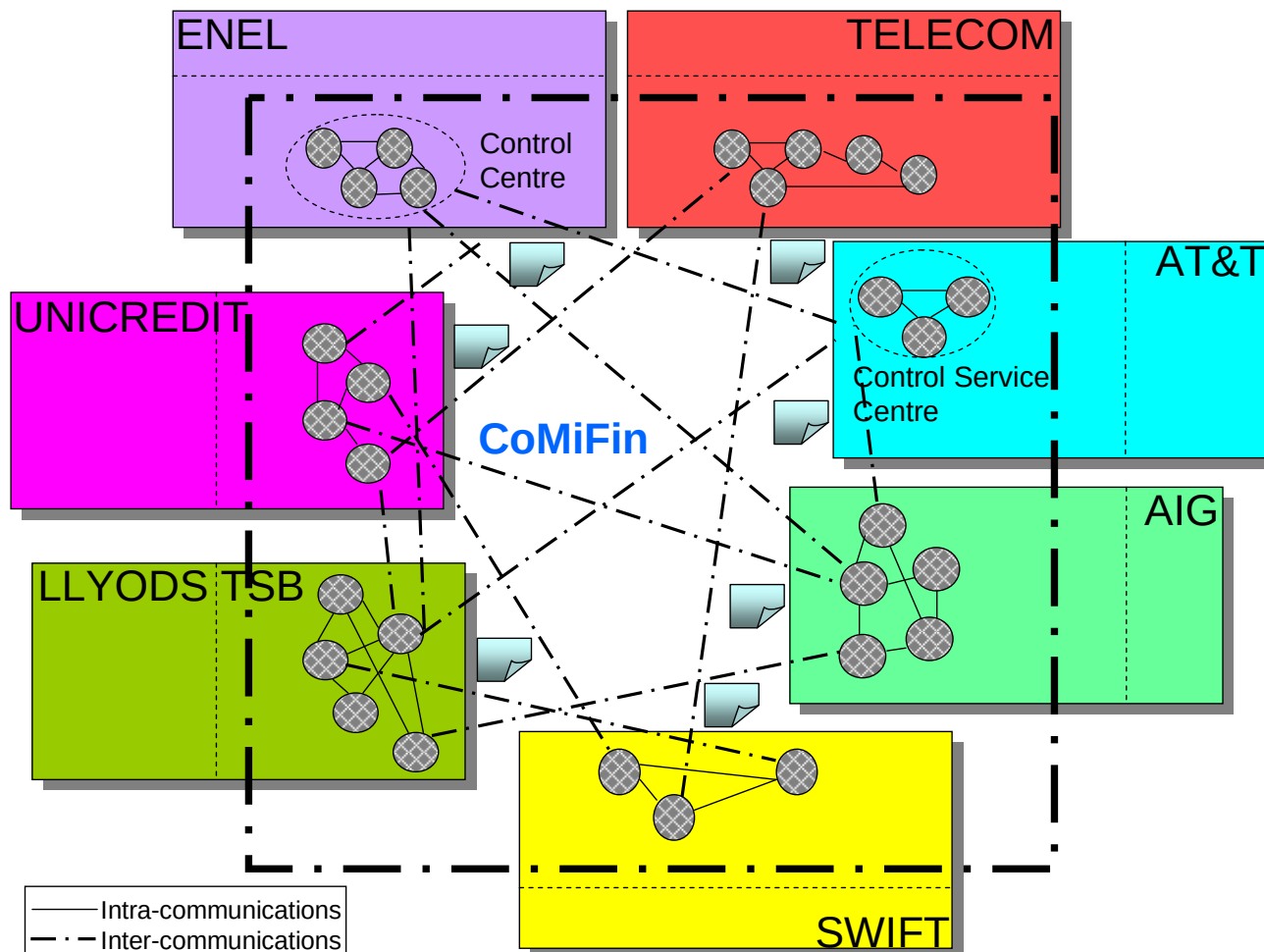
Esettanulmány: CoMiFin

- „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

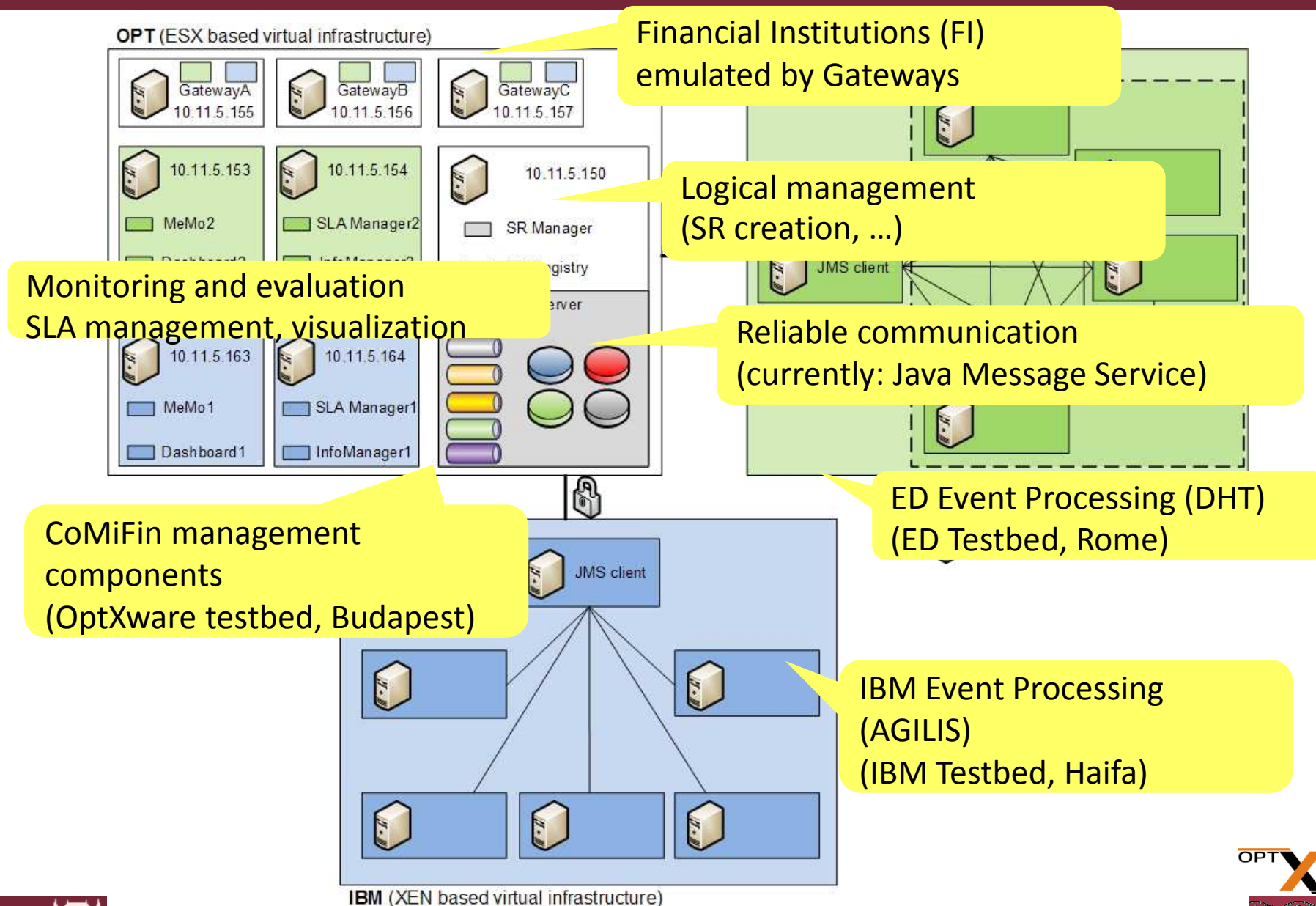
Példa: magyar infrastruktúra



Logikai architektúra



Architektúra



Eredmények megjelenítése

JBoss Portal 2.7.2-GA - Mozilla Firefox

http://10.11.5.153:8080/portal/auth/portal/Dashboard/6_AlertList

Alert details (time, source, target, etc.)

Logged in as: sr_manager

Home S_SR_Manager_Page 6_AlertList

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	Service10	9X.16X.X5X.X24	-0.1909274
2010-07-01 10:07:09.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service11	19X.X1X.X0X.X05	-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

Service effected

Score on the alert

Done

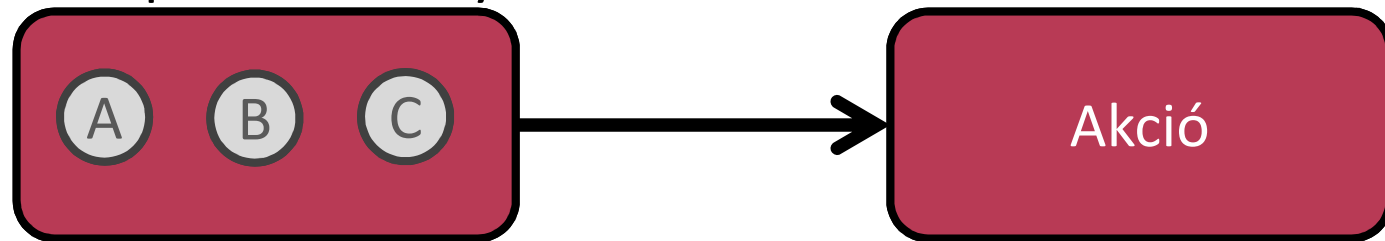
Modellalapú fejlesztési módszer komplex események feldolgozásához

Motiváció

- Események feldolgozása – alapja: a mintafelismerés
 - Az érdekes események összetettek lehetnek
- Komplex esemény: elemi eseményekből álló struktúra
 - Complex Event Processing – CEP
- Példák
 - „A webserverver terheltsége 90% és az adatbázis serveren lekérdezést futtatnak.” $\Rightarrow$ „Vonjunk be tartalék erőforrást.”
 - „Az X részvények értéke jelentősen csökkent, és a vele korreláló Y részvények is elkezdtek esni.” $\Rightarrow$ „Adjunk el Y részvényeket.”

A

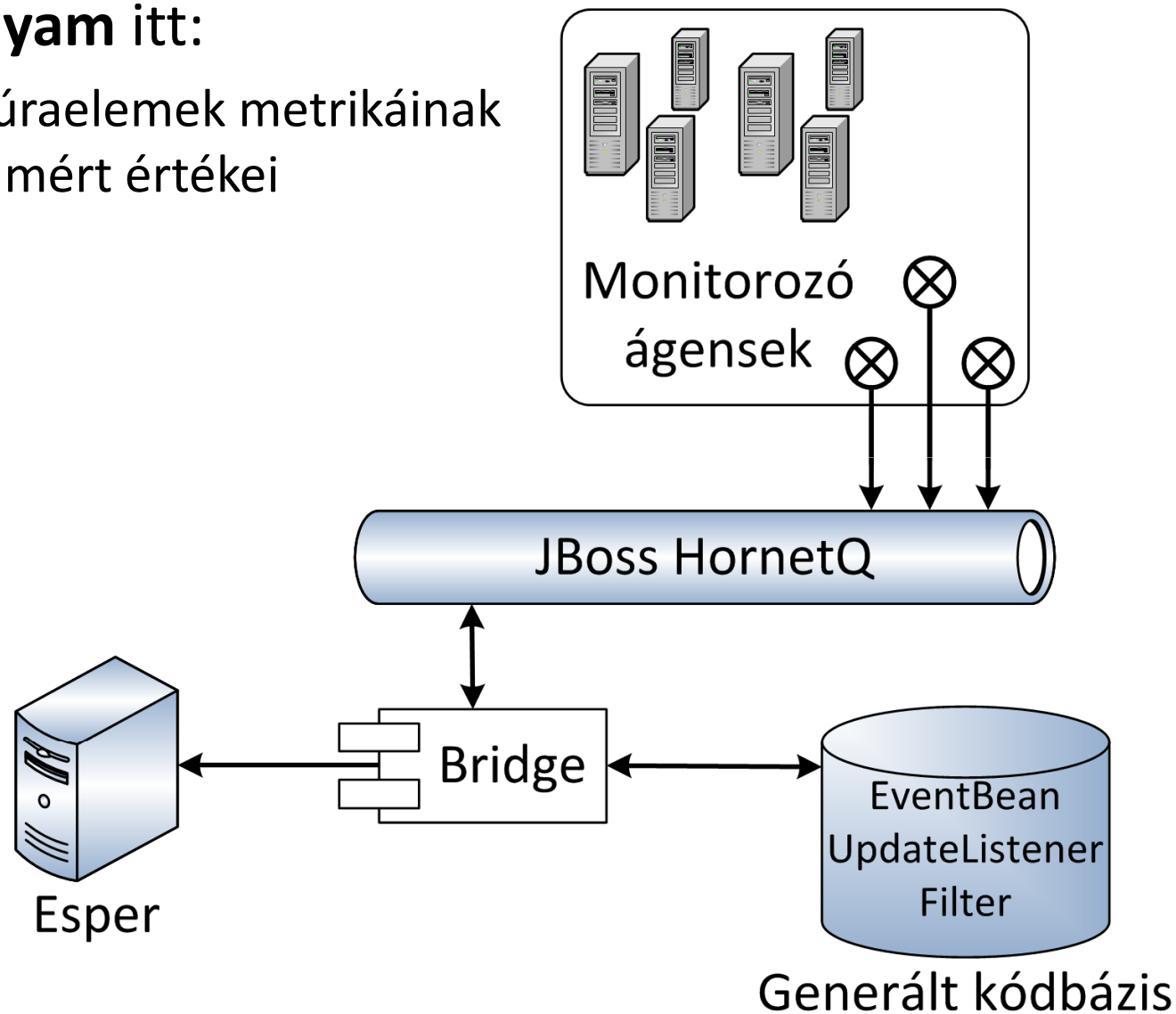
Komplex esemény



Mintakörnyezet

Szimulált IT infrastruktúra

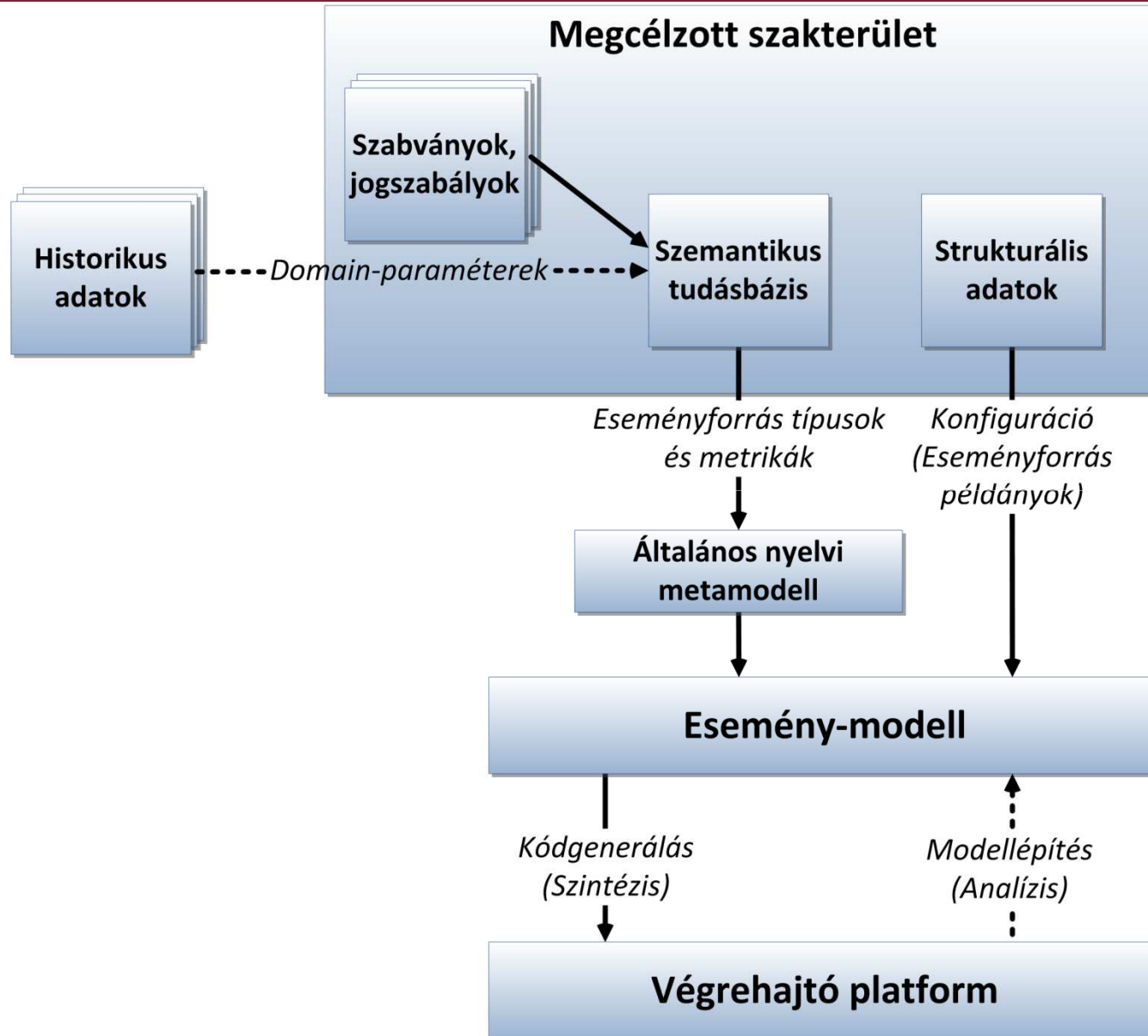
- Az **eseményfolyam** itt:
 - Az infrastruktúraelemek metrikáinak folyamatosan mért értékei



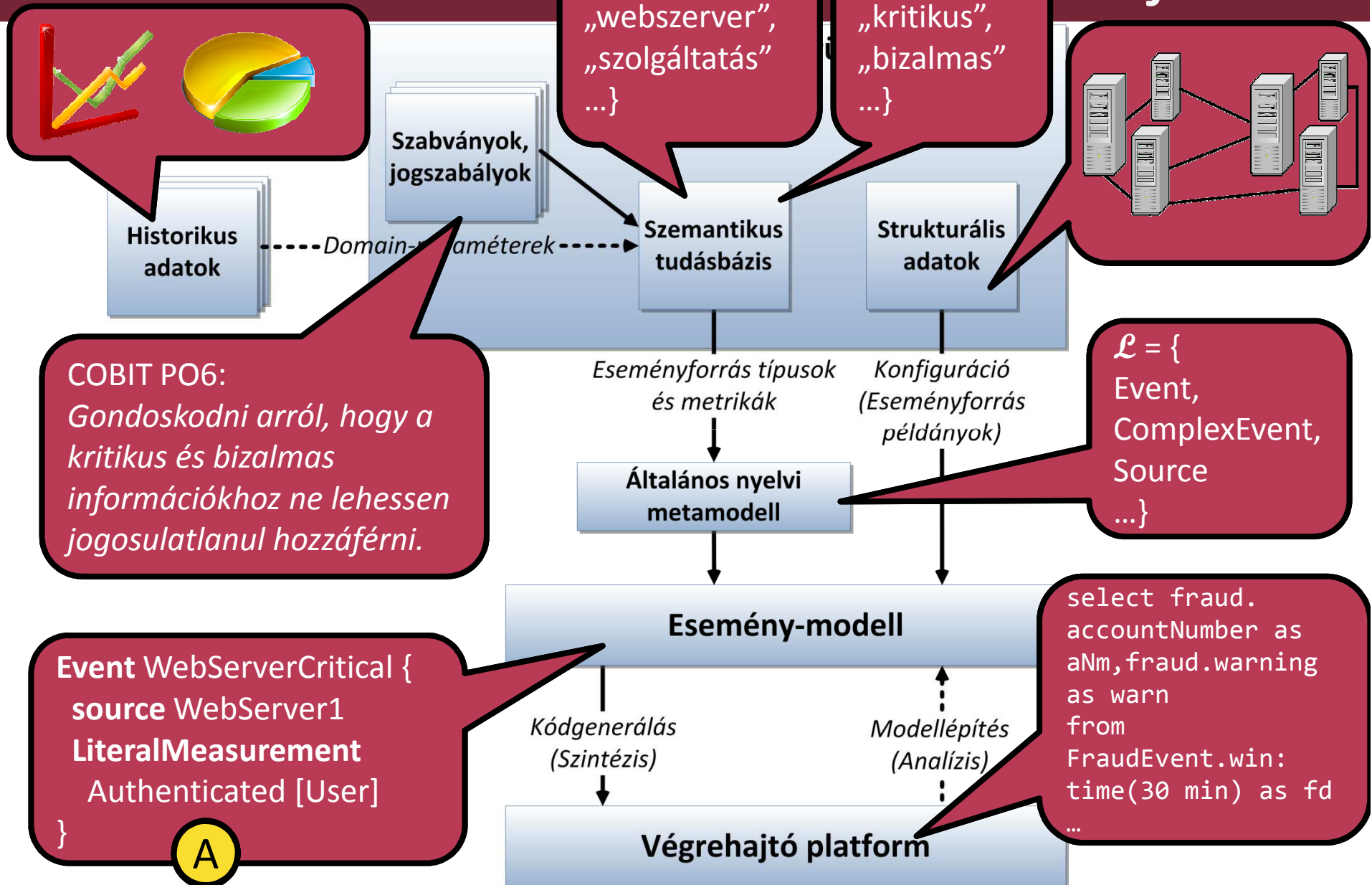
Problémafelvetés

- Különböző platformok, saját nyelvvel – nincs közös szabvány
- Nehezen kezelhetőek a nagy eseményminták
 - Platformközeli nyelv → sok „kézi kódolás”
 - Egymást fedő eseményminták problémája
- Magas szintű követelményeknek való megfelelés biztosítása
 - Ad-hoc konfigurációk
 - Eseti hibakezelés
 - Heterogén információforrások
- Modellalapú megközelítés
 - Magasabb logikai szinten történő ellenőrizhetőség
 - Generált kód → a szintaktikai hibák megszüntethetőek
→ több célplatform is megcélozható egy modellel

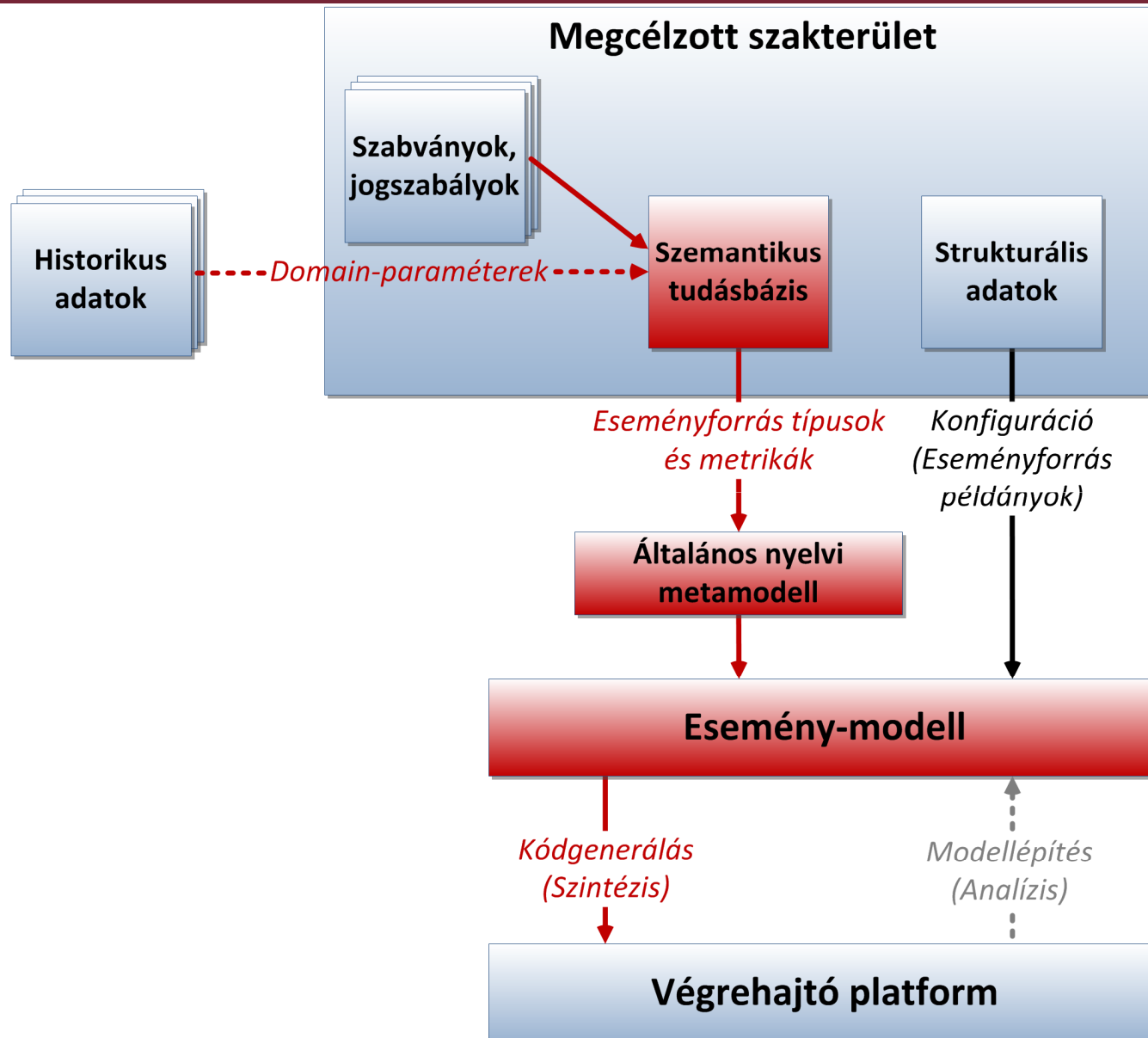
A kialakított megoldás struktúrája



A kialakított ikt. sz. úrája



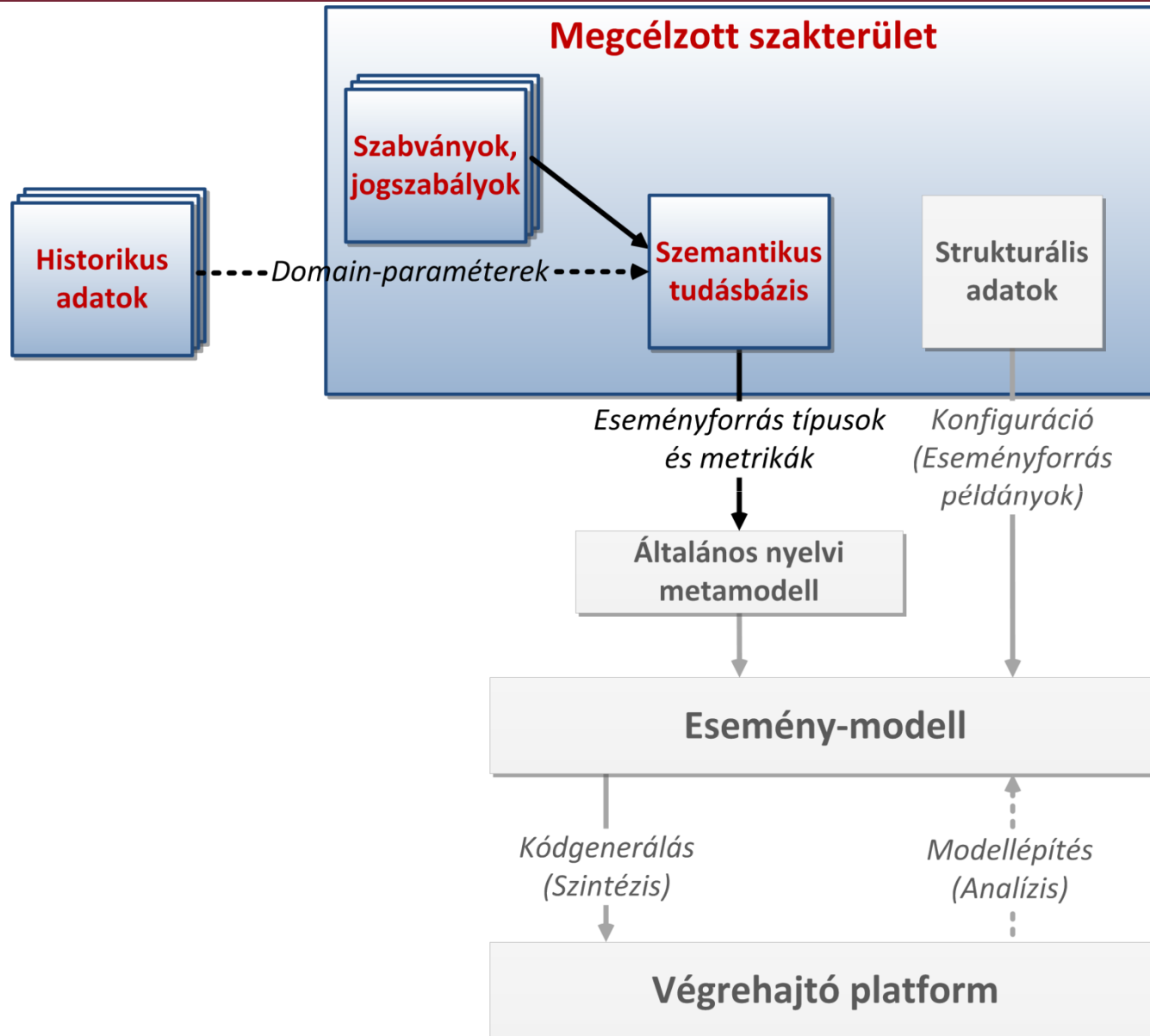
Elkészült



Elkészült

- Módszer a magas szintű követelmények formalizálására
- Módszer a historikus adatok felhasználására
- Szemantikus tudásbázis mintaséma
- Módszer a szemantikus adatok kinyerésére
- Modellezőnyelv prototípus
- Fejlesztőeszköz prototípus
 - Modellvalidáció
 - Kódgenerálás

Szemantikus tudásbázis

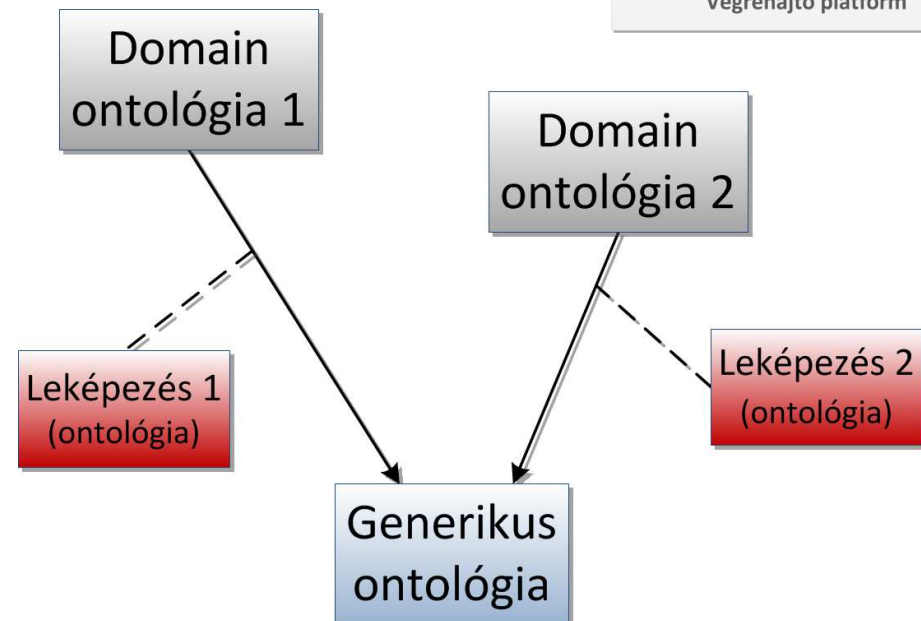
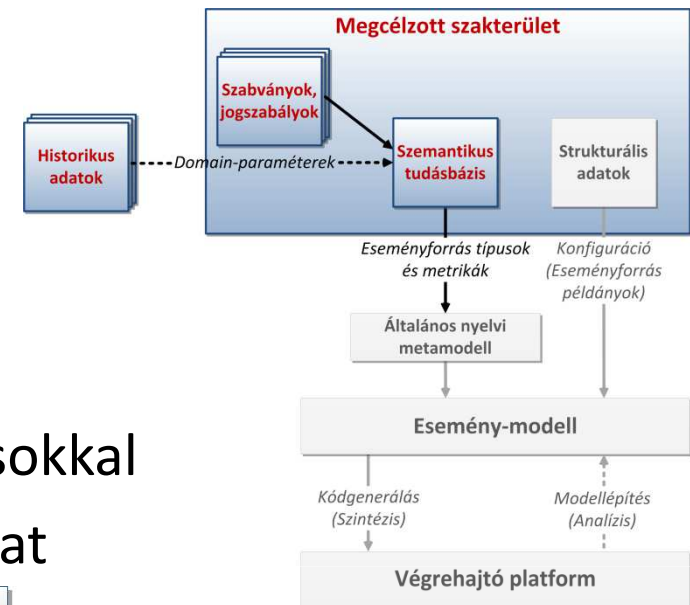


Szemantikus tudásbázis

- Jellemző gyakorlati probléma:
(túl) sok mérhető metrika
- Jó lenne formalizálni a
magas szintű követelményeket
 - Ezeket pedig összekötni a mérhető metrikákkal
- Szemantikus tudásbázis: egy ontológia
 - Következtető logikákkal kimutatható összefüggések
 - „*Létezik-e minden X kritikus erőforráshoz két példány, amelyek közötti kapcsolat a Tartalék típus példánya? Figyeljük meg ezeket.*”
- A szemantikus tudásbázis tehát:
 - Lehetőséget nyújt a magas szintű kritériumok formalizálására
 - Lehetőséget nyújt bizonyos szintű ellenőrzésekre

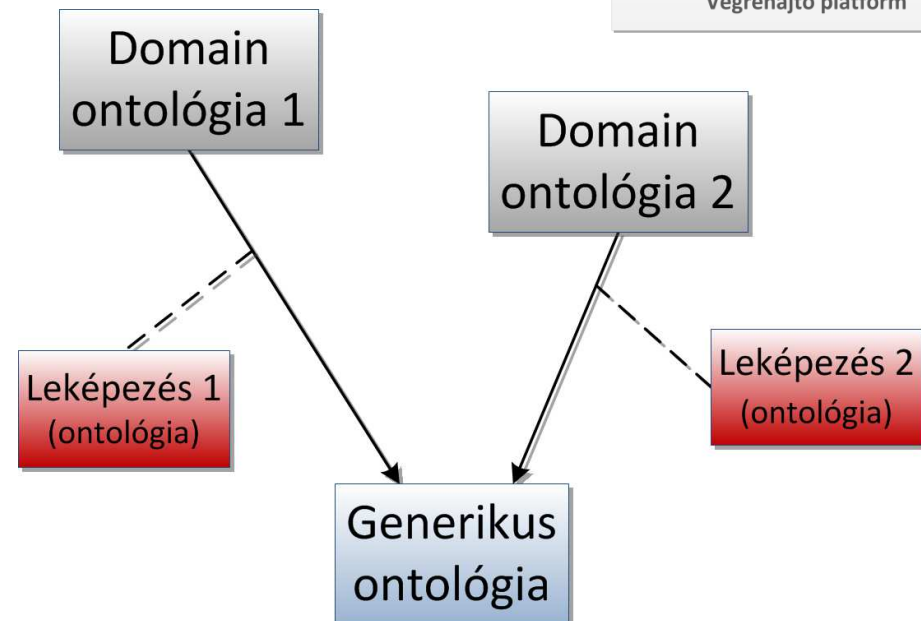
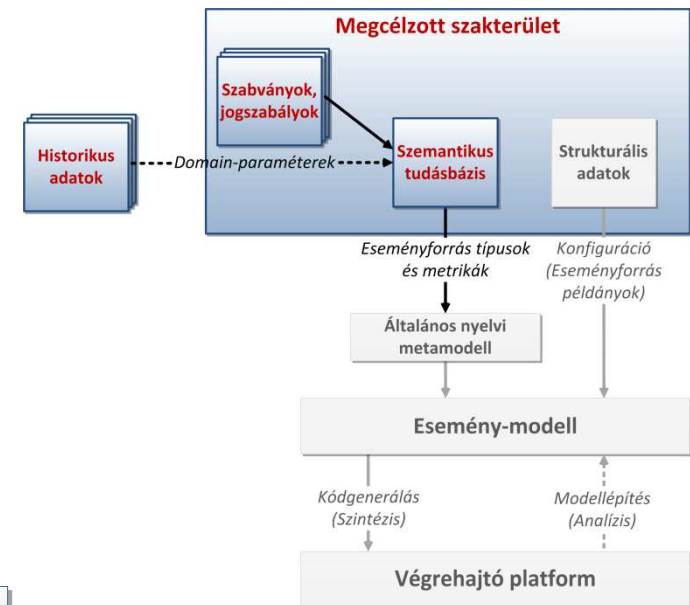
Szemantikus tudásbázis

- Domain ontológia
 - Az adott szakterületet írja le
 - Minden szakterületen más
- Generikus ontológia:
 - A modellező nyelv alapján, rögzített típusokkal
 - Erre lehet leképezni a domain ontológiákat
 - Minden esetben azonos

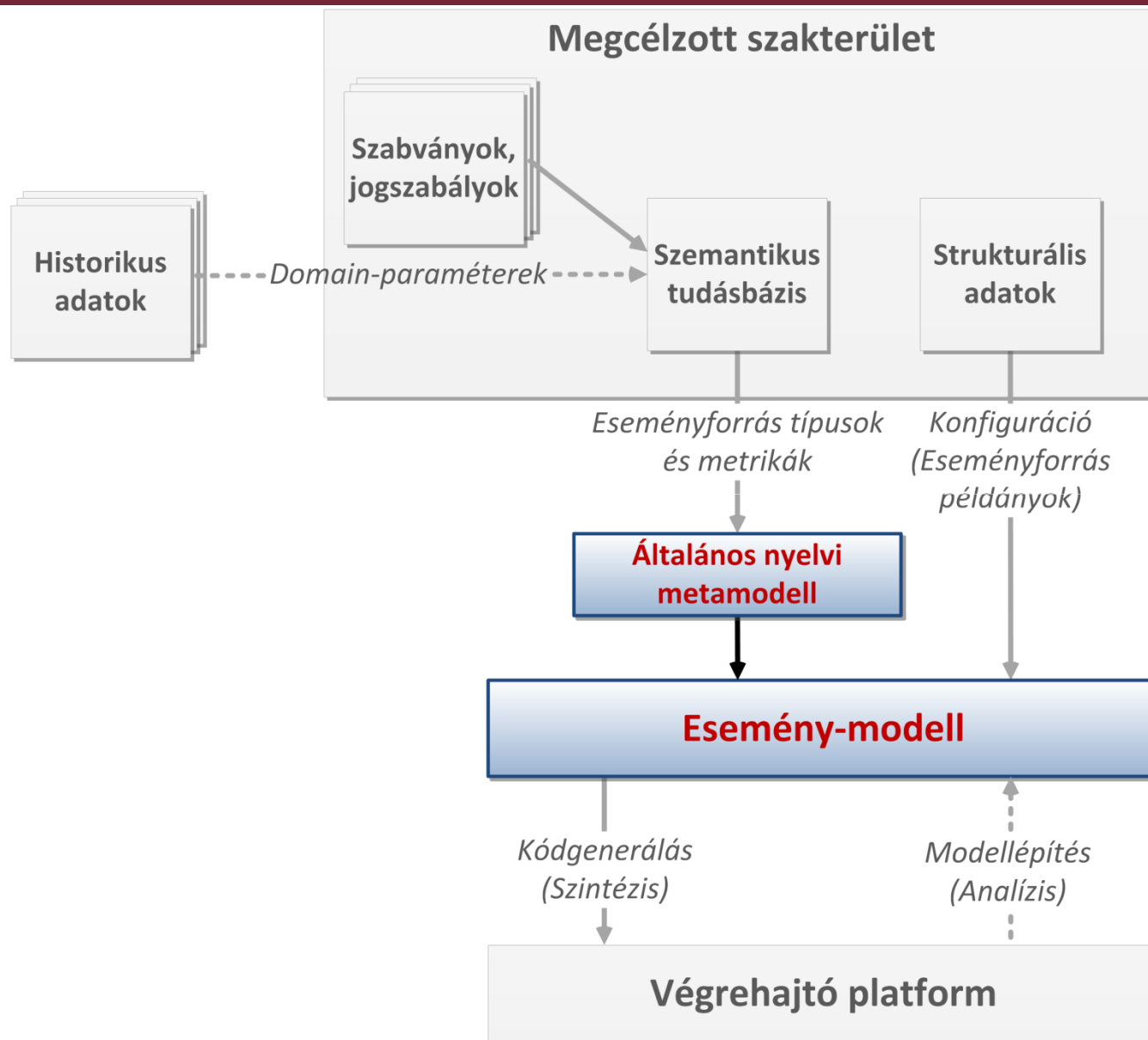


Szemantikus tudásbázis

- Példa leképezések (IT):
 - Webszerver $\Rightarrow$ *SourceType*
 - Terheltség $\Rightarrow$ *Quantifier*
 - $m(\text{Webszerver}, \text{terheltség}) \Rightarrow$ *Metrics*
 - $\text{kritikus}(m, [0.9;1]) \Rightarrow$ *Qualifier*



Complex Event Description Language



Complex Event Description Language

- Szakterület-független modellre épül
- A szakterület információival egészül ki
 - Eseményforrás típusok (*webszerver*)
 - Eseményforrás példányok (*a Server1 webszerver*)
 - Metrikák (*kritikus processzor terheltség $\geq 90\%$*)

Szakterület-független
nyelvi elem

Szakterület-specifikus
információk

- **Event** CPUloadCritical {
 source Server1
 PercentageMeasurement CPUload **Minimum** 90
}

Complex Event Description Language

- Nyelvi alapok:

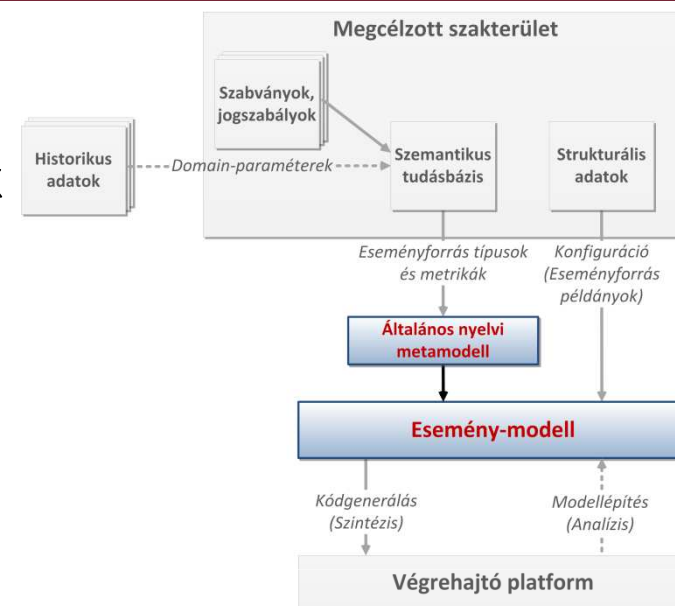
- Komplex operátorok az elemi események relációinak leírásához:

EXISTS, FOLLOWS, CONCURRENT

- Időablak – TIMEWIN(T)

- Ezen felül még:

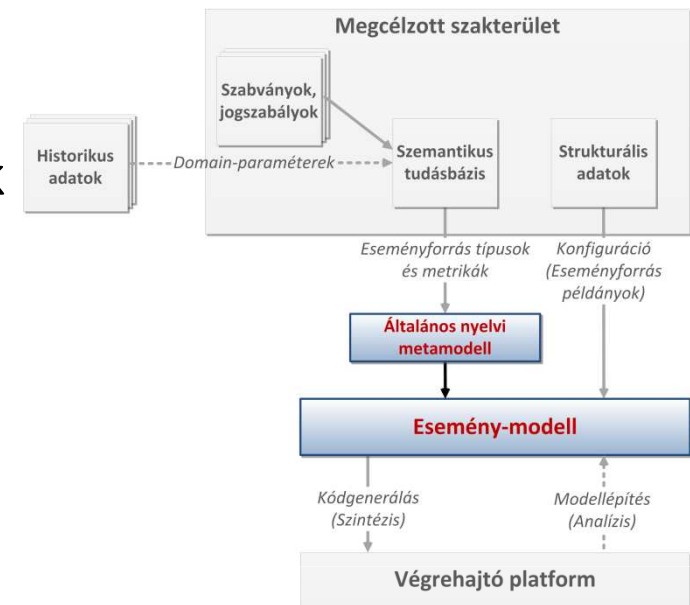
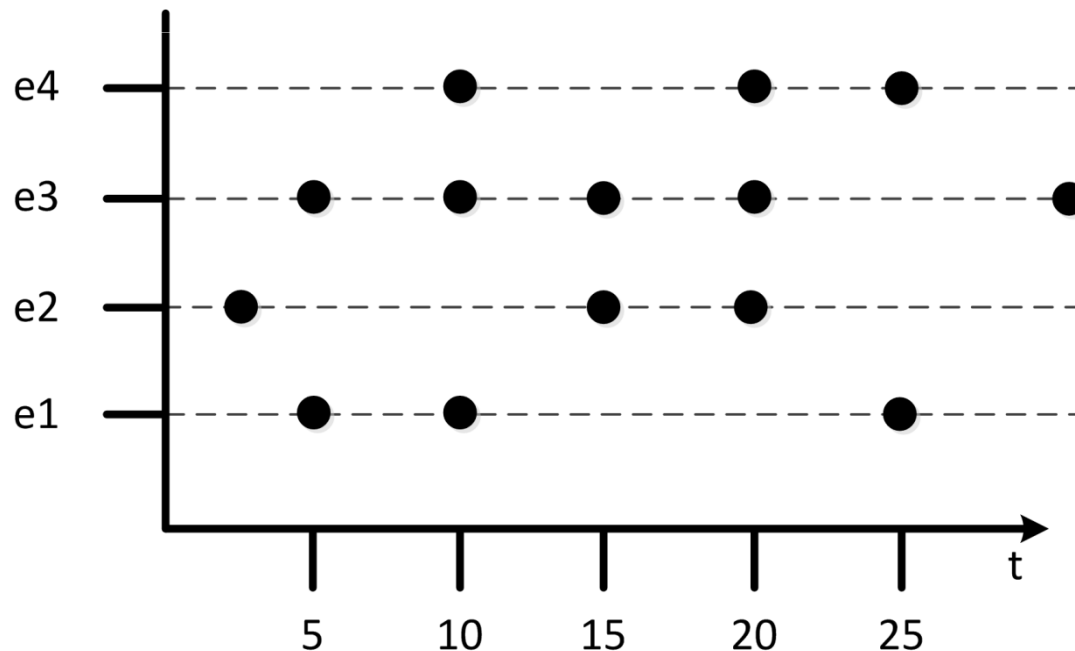
- Aggregációk
- Strukturális tervezési minták (OO-szerű)
- Végrehajtható akciók
- Minták alkalmazása erőforrások csoportjaira
- Többféle metrika: százalék, skalár, szöveges, intervallum
- Névterek kezelése, telepítési konfigurációk kezelése
- Környezeti (nem-funkcionális) paraméterek kezelése



Complex Event Description Language

■ Nyelvi alapok:

- Komplex operátorok az elemi események relációinak leírásához:
EXISTS, FOLLOWS, CONCURRENT
- Időablak – TIMEWIN(T)



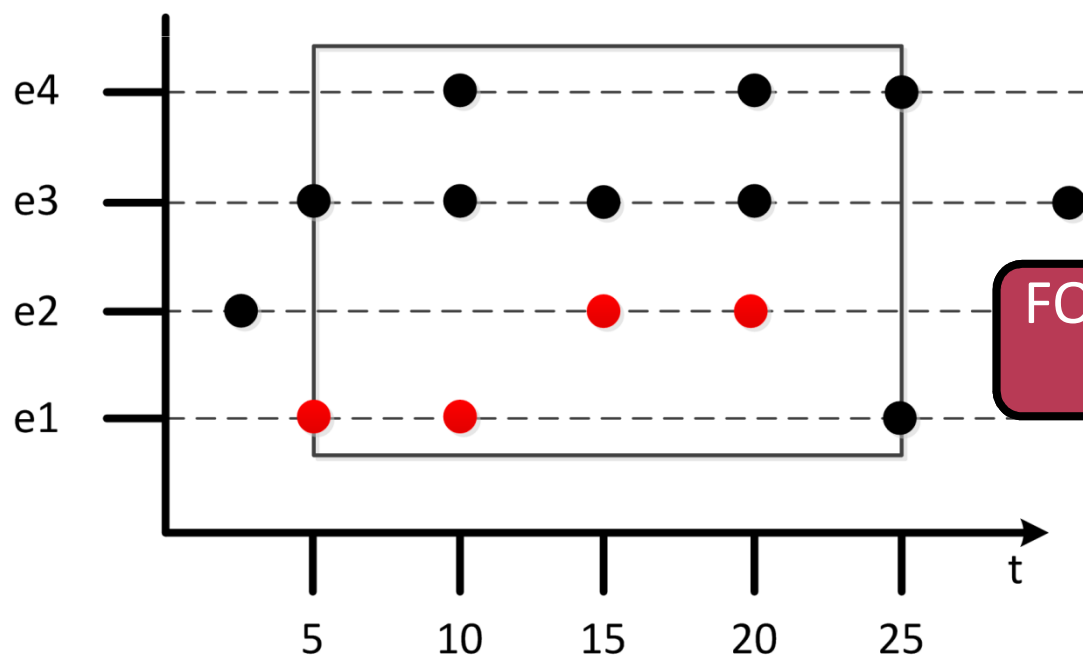
Complex Event Description Language

■ Nyelvi alapok:

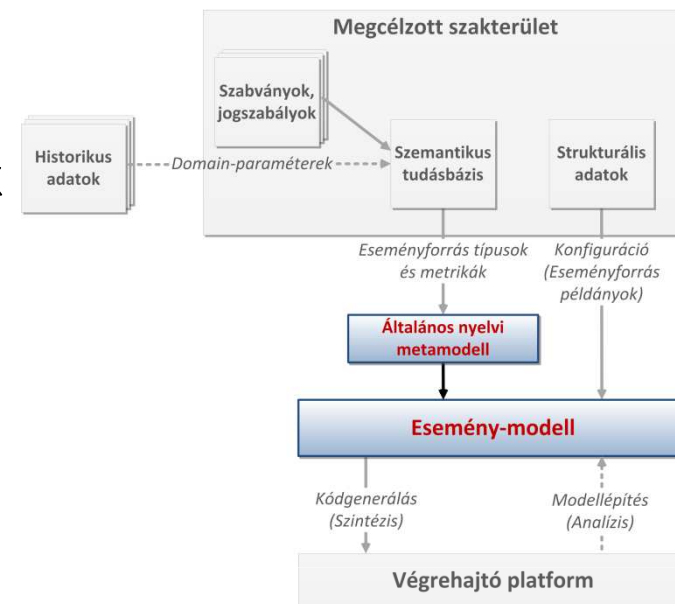
- Komplex operátorok az elemi események relációinak leírásához:

EXISTS, FOLLOWS, CONCURRENT

- Időablak – TIMEWIN(T)



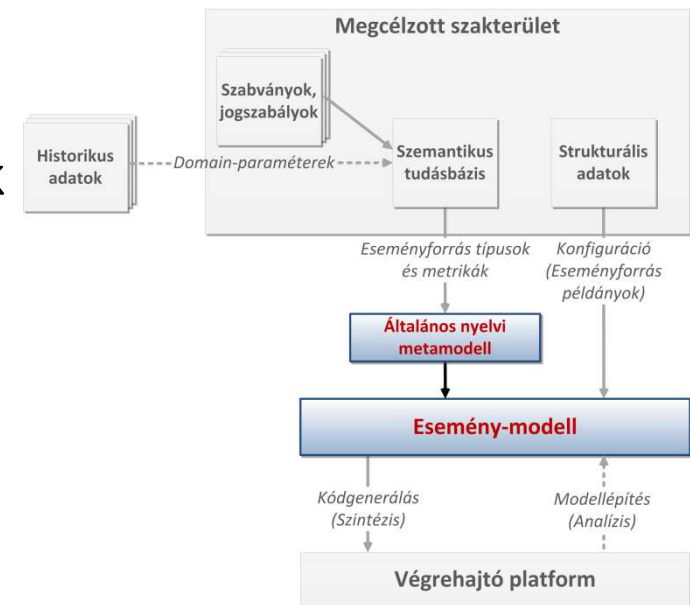
**FOLLOWS_T(e1(2), e2(2);
T: Maximum 20)**



Complex Event Description Language

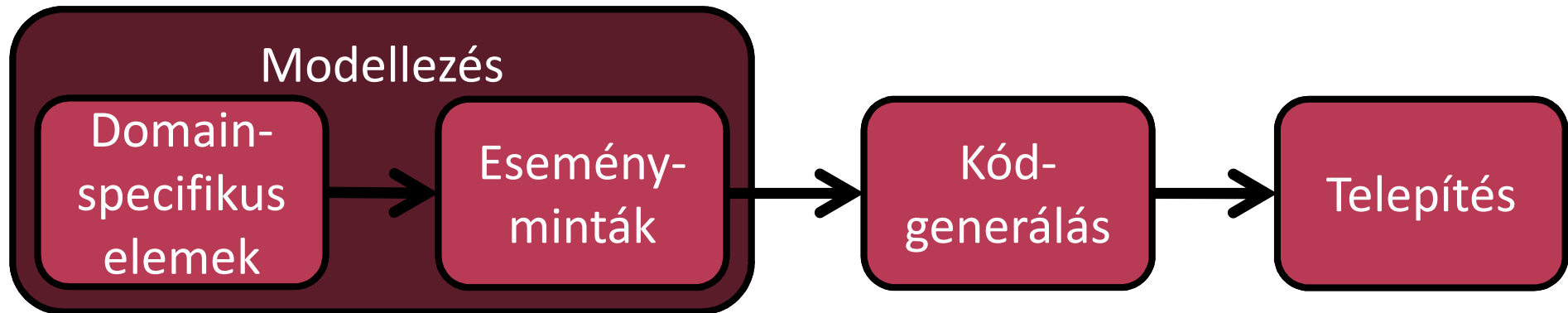
- Nyelvi alapok:

- Komplex operátorok az elemi események relációinak leírásához:
EXISTS, FOLLOWS, CONCURRENT
- Időablak – TIMEWIN(T)



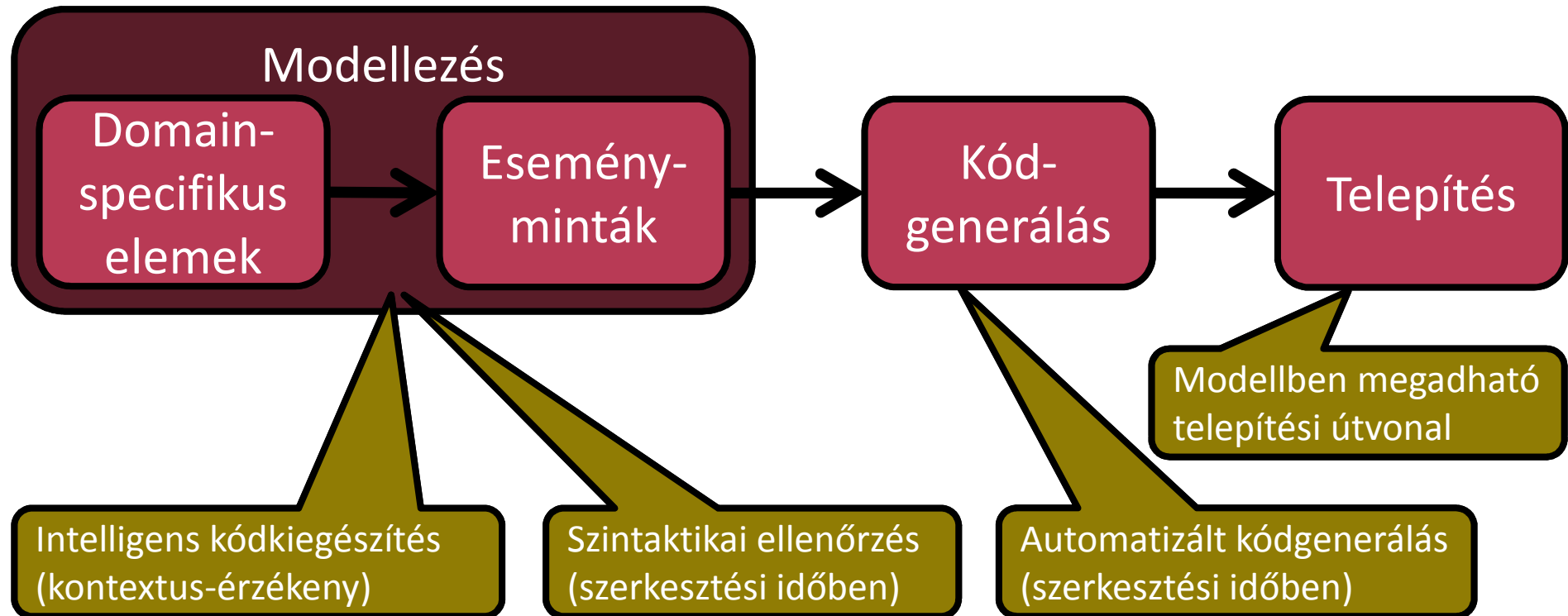
- **ComplexEvent** CriticalServer {
 CONCURRENT_T(CPULoadSuspicious,
 BackupLoadSuspicious; **T: Minimum 30**)
 action {
 Action of Type sendWarning
 }
}

Tervezési-fejlesztési munkafolyamat



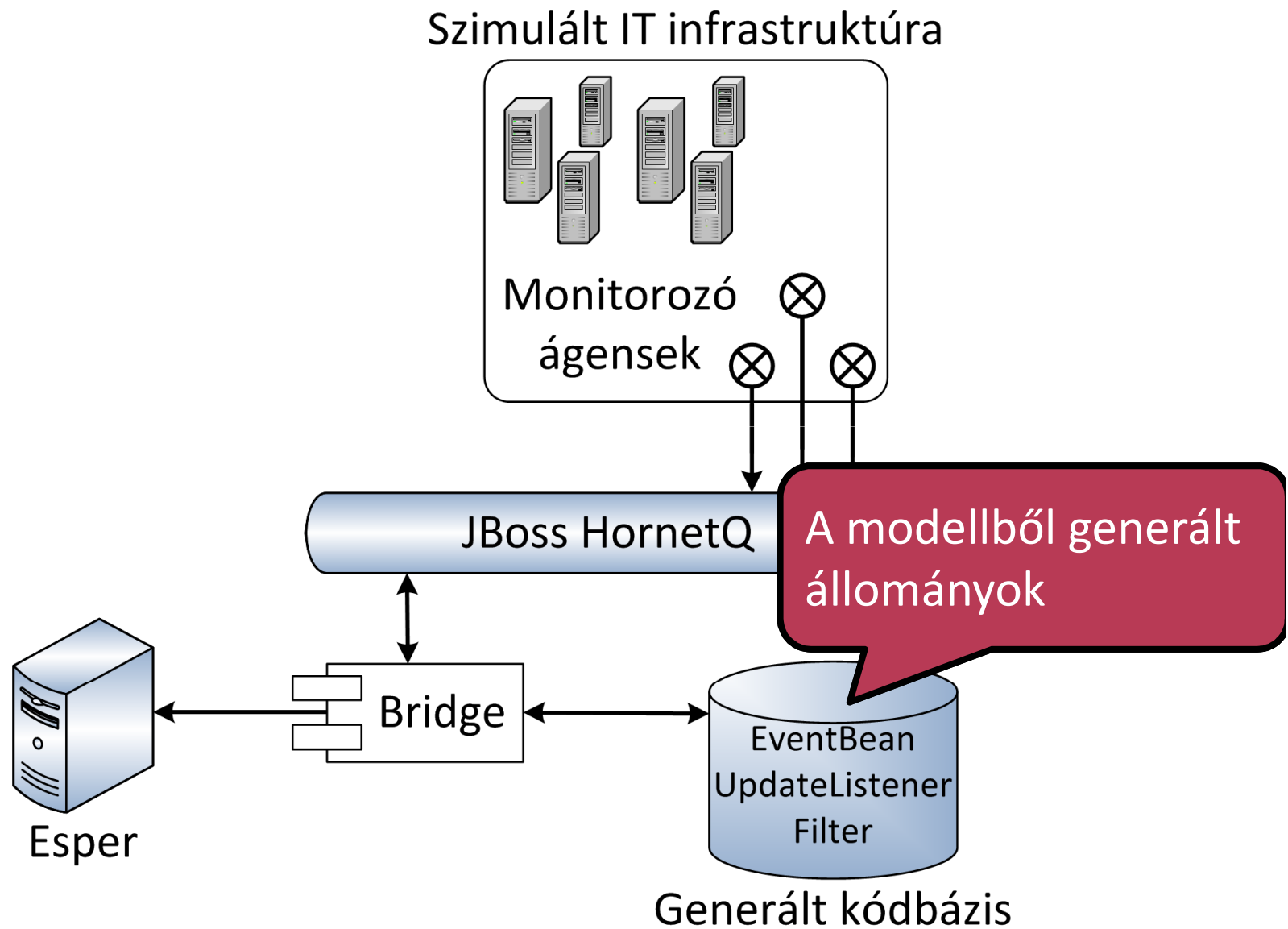
- Generált kód: nem csak eseményminta definíciók!
 - Esemény-definíciós osztályok (*EventBean*), feldolgozást végző osztályok (*UpdateListener*), interfész definíciók, konfigurációs állományok
 - Mindezt **egy** modellben definiáltuk
- Esper esetében: háromszor több utasítás a generált kódban, mint a modellben
 - Nagyobb rendszereknél ez az arány várhatóan növekszik

Integrált fejlesztőkörnyezet



- Domain-specifikus fejlesztőeszköz
- Kifejezetten komplex események modellezéséhez
- A munkafolyamat támogatása több ponton

Tesztkörnyezet

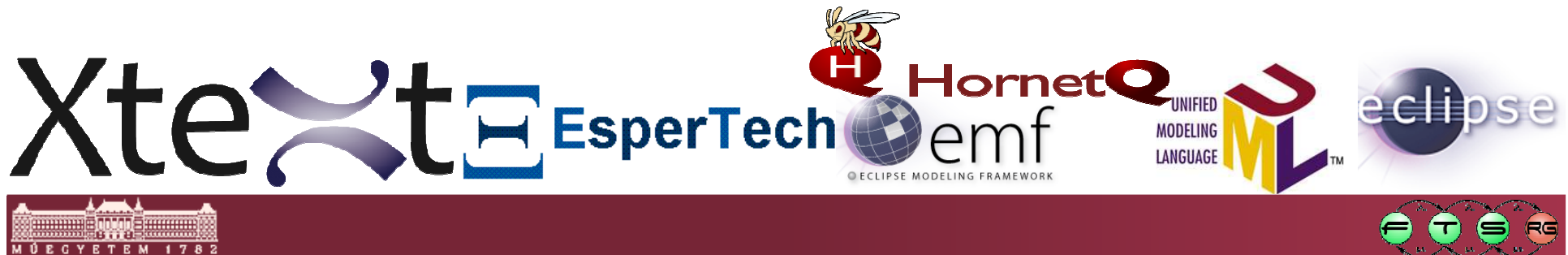


Továbbfejlesztési lehetőségek

- Analízis és integráció támogatása
 - Modell létező kódbasisból
- Grafikus felület
- Proaktív irányítórendszerek fejlesztésének támogatása
 - Historikus adatok visszacsatolása a szemantikus tudásbázisba
 - Valós idejű intelligens feldolgozás (klaszterezés, osztályozás)
 - Lásd: MAPE-K szabályozás
 - Példa alkalmazás: algoritmikus kereskedés modellalapú támogatása

Összefoglalás

- Bővíthető, szakterület-független eseménymodell
- Modellezőnyelv (Complex Event Description Language)
- A szakterület információinak ontológia-alapú kezelése
- Módszer a magas szintű követelmények ellenőrzésére
 - Szabványkonformitás, jogszabályoknak való megfelelés
- Integrált fejlesztőkörnyezet
 - Szintaktikai támogatás, kódgenerálás...



54. dia

g1

vagy nagyobb logók, jobban szétszórva, vagy még egy sor jöhet
goerenh; 2011.11.08.

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-fejlesztési>
- <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://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>