Hansken job scheduler:
Definition of business rules according to the MBRM framework

Date: July 6th, 2012
Supervisor: Dr. M. Worring (UvA), R. van Baar (NFI)
Table of contents

- Introduction
  - Digital investigation process
- Problem definition
- MBRM method
- Business rules
  - Theory
  - Requirements
  - Rules
- Business rules management system (BRMS)
  - Requirement principles
- Conclusion
- Recommendations
- Questions
IN 60 SECONDS:

- 1 NEW DEFINITION ADDED ON WIKIPEDIA
- 1,600+ READS ON SCRIBD
- 13,000+ HOURS MUSIC STREAMING ON PANDORA
- 12,000+ NEW ADS POSTED ON CRAIGSLIST
- 370,000+ MINUTES VOICE CALLS ON SKYPE
- 98,000+ TWEETS
- 20,000+ NEW POSTS ON TUMBLR
- 13,000+ IPHONE APPLICATIONS DOWNLOADED
- 100+ NEW LINKEDIN ACCOUNTS
- 100+ NEW ARTICLES PUBLISHED
- 1 NEW CONTENT ADDED ON ANSWERS.COM
- 600+ NEW VIDEOS FROM YOUTUBE
- 70+ NEW DOMAINS REGISTERED
- 60+ NEW BLOGS
- 168 MILLION EMAILS ARE SENT
- 694,445 SEARCH QUERIES
- 1,700+ FIREFOX DOWN LOADS
- 695,000+ FACEBOOK STATUS UPDATES
- 50+ WORDPRESS DOWN LOADS
- 125+ PLUGIN DOWN LOADS
- 510,040 WALL POSTS
- 79,364 COMMENTS
Introduction: digital investigation, anno 2014:

In the Netherlands, based on current case statistics from the NFI:

Number of police agency’s: 10
Cases: 1,000 per agency, per year
Average case size: 4,000 GB (min: 1MB, max: 200TB)
Retention time: 6 months

Storage capacity needed: 200,000,000 GB = 20,000 TB = 20 PB of case data a year
8 Gb data-upload per second (resulting in 3 PB of trace indexes every year)

Data to process: 110,000 GB = 110 TB of case data a day
15 Gb data processing per second (resulting in 16 TB of trace indexes a day)
The ‘old fashioned’ process of a digital investigation

1. **Seizure**
   - Imaging

2. **Securing**
   - Imaging

3. **Processing**
   - Technical detective

4. **Reporting**
   - Analyst

5. **Analysis**
   - Tactical detective
The process of a digital investigation as a service

**Save valueable time!**

The process of a digital investigation as a service involves the following stages:

1. **Seizure**
2. **Securing**
3. **Processing**
4. **Analysis**
5. **Collaborate**

- **Digital storage**
- **Virtuel research environment**
- **Analyst**
- **Technical detective**
- **Tactical detective**
Problem definition

- How should job scheduling principles be handled within Hansken?

  • Usage of business rules
    • How to capture and define business rules?
      • Methodology?
    • What rules should be defined?

  • Use a business rules management system (BRMS)!
    • What are its requirements?
Problem definition ⇒ an example

- Murder case
- Fraud case
- Child pornography case

Trace indexing
Problem definition → an example (2)
Problem definition → an example (3)
Method

• Several rule management methods were assessed:
  • BRADES, SSADM and ERM-extensions but found to less suitable compared to MBRM.

• Usage was made of the Manchester Business Rule Management (MBRM) framework
  • Has proven its usefulness in similar large scale projects
  • Allows for traceability from rules to system components: transparency
  • Provides structural consistency for expressing and grouping rules
Method

**Intentional rules**

- A car with accumulated mileage greater than 5000 since its last service must be scheduled for service.

**Operational rules**

- If \( \text{Car.miles-current-period} > 5000 \) then invoke \( \text{Schedule-service (Car.id)} \) End if

**IS architecture rules**

- Identical to operational rules, but in accordance with the system architecture (out of scope)
Business rules - theory

‘Defines or constrains some aspect of a business’ – IBM

- Should aid the organization in achieving its goals
- Express policies within an organization using a formalized vocabulary
Business rules – advantages

• Separate IT-architecture from variable business aspects

• Lowers the cost incurred in modification of business logic

• Rules are externalized, easily shared amongst applications

• Give rule authority back to business analysts

• Automation of business processes; save time
Business rules

For what business processes must rules be applied?

- Case priority
- Tool priority
- Case scheduling
- Quick indexing options
- Resource allocation / load distribution
- Priority themes
- Event job validation
- Alert generation
- Event logging → chain of evidence
- Trace indexing / a-synchronous query processing

\[
\text{if} \quad \text{suspect hold time} \leq 48 \text{ hours} \\
\text{then} \quad \text{start quick scan}
\]
Business rules management system - theory
Business rules management system - requirements

The following requirement principles have been established:

- Privacy
- Security
- Reliability
- Transparency
- Stability
- Performance
- Compatibility
- Flexibility
- Scalability

- It is likely that the system will be implemented beyond The Netherlands
Conclusion & recommendation

- This project has provided the NFI with a knowledge of:
  - How to capture and define business rules with the application of a scientific method
  - Specific set of business rule (statements)
    - How to manage business rules using a BRMS
  - Operational rules → to IS-architecture rules → implementation
    - Format to RIF-standards (W3C) or vendor specific rule language (DRL, IRL)
    - Choice for a specific BRMS system, based on requirement principles
Questions?

Company Rules:
1) THE BOSS IS ALWAYS RIGHT
2) IF THE BOSS IS WRONG REFER TO RULE 1.

© Original Artist