



Decision engine and ontologies: a way toward autonomic system management

Maurice Israël - Thales Communications

Land & Joint Division

Table of Contents

Functional Architecture

- Monitoring
- Policy Based Management
- Monitoring demo
- Reconfiguration solutions
- Dynamic invocation

Focus on semantics

Focus on reconfiguration algorithms

- Status graph
- Inference engine

Conclusion

Une panne informatique paralyse le réseau de Bouygues Telecom

Christophe Guillemin, publié le 17 novembre 2004
 Tags: Technologie, Téléphone Mobile, Réseaux et télécoms

Mis à jour - Le réseau téléphonique national de l'opérateur mobile a été victime d'une panne informatique qui a bloqué l'émission et la réception des appels. Deux serveurs centraux fonctionnant en relais sont tombés en panne simultanément.

Ce mercredi matin à 6 heures, les abonnés de Bouygues Telecom ont constaté avec surprise qu'ils étaient dans l'impossibilité de passer ou de recevoir tout appel.

GOVERNMENT AGENCY WEBSITE RE-HACKED Taipei, Aug. 12 (CNA) The website of the National Assembly was hacked Thursday for the second time in a week, causing the paralysis of a mainframe computer.

It is believed that the National Assembly's website was hacked by a mainland Chinese computer specialist following a previous intrusion Tuesday, in which some files were replaced. Thursday's attack was more serious however, as viruses introduced into the system by the hacker damaged computer

3 Land & Joint Division

On Monday, March 10, IBM's technical division was performing a routine replacement of a defective electrical unit in an IBM disk system, type RVA (the disk system used for storage of data in DB2 database software), at DMdata's operating installation in Ejby. During the repair process, there was an electrical outage in the disk system, and the result was that operations stopped at one of the Bank's two operating centres (Ejby) as of 16:08 CET

November 01, Associated Press — Exchange resumes activity. The Tokyo Stock Exchange

(TSE) suspended trading in most stocks and bonds the morning of Tuesday, November 1, following a glitch in its transactions system, but was able to resume activity for part of the

afternoon session.



Nouvelle panne informatique à la SNCF

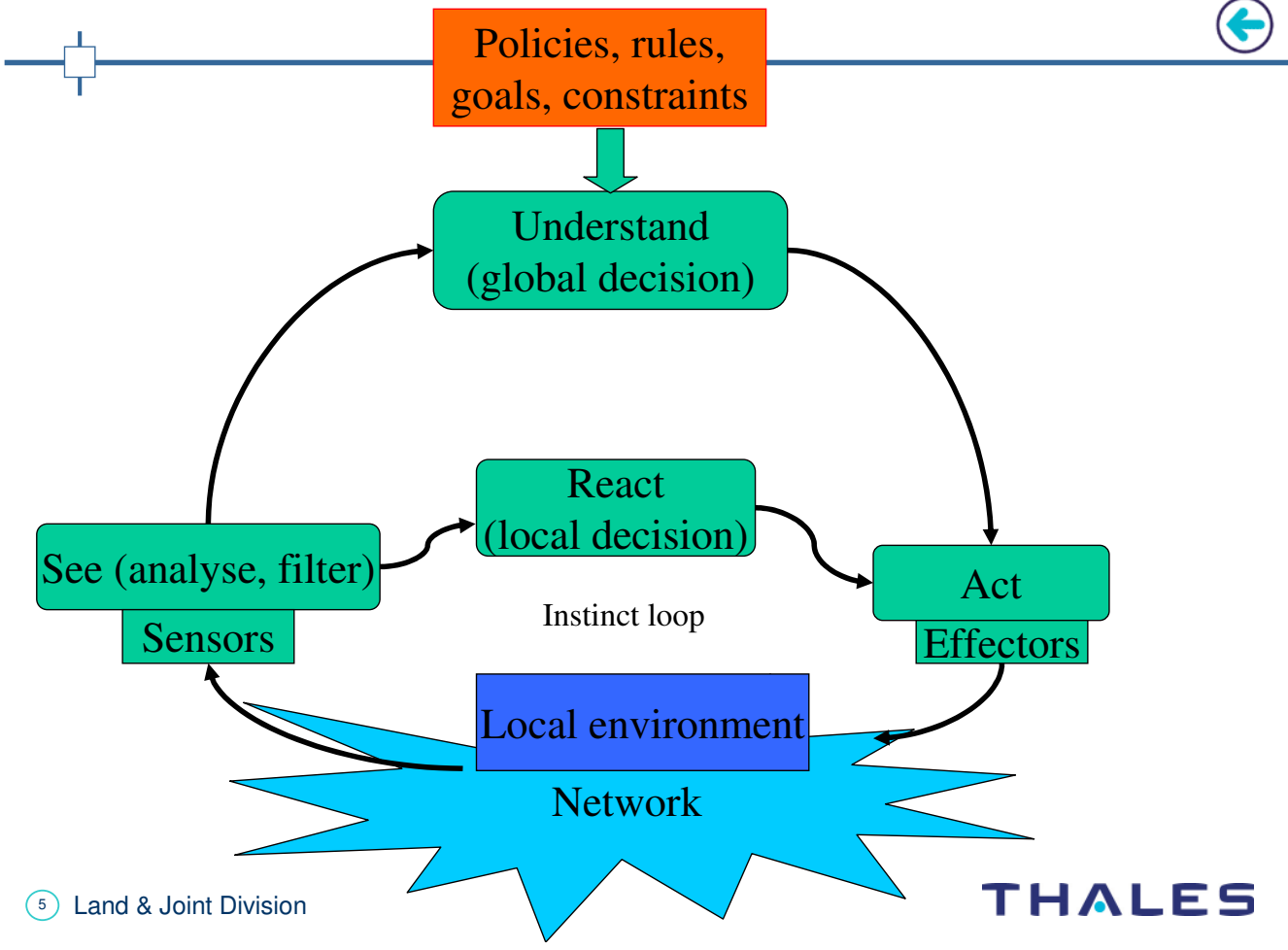
03-12-2004
 Par la Rédaction

800 terminaux de vente sur 4.000 ont été paralysés pendant plus de 24 heures

Publicité Ca commence à faire beaucoup. La SNCF a été une nouvelle fois victime

We aim at improving existing and exploiting enabling technologies to response to the set of problems of network management automation.

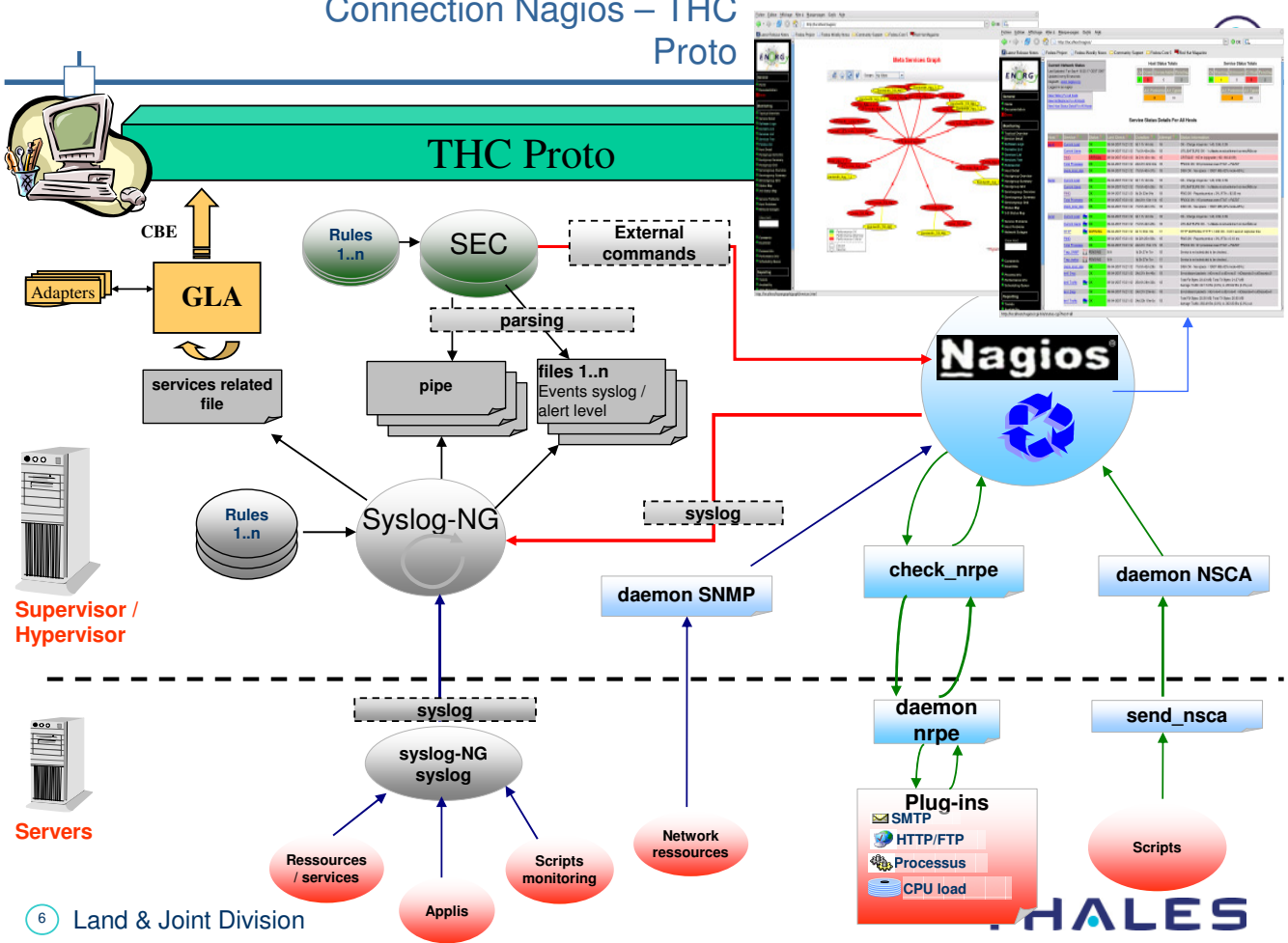
The essence of Autonomic Management is the ability for a system to self-govern its behavior within the constraints of business goals that the system as the whole try to achieve



5 Land & Joint Division



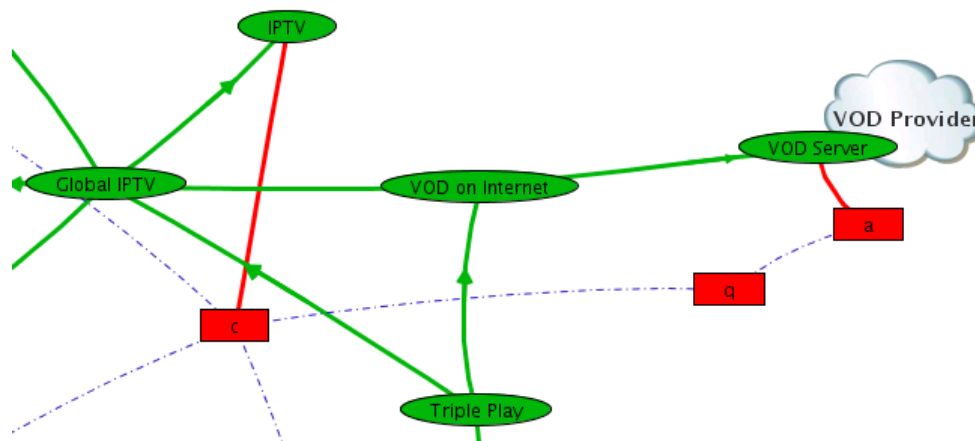
Connection Nagios – THC Proto



6 Land & Joint Division



To monitor business goals, the demonstrator provide tools to **create, describe, link** high-level services based on other services and/or network resources.



7 Land & Joint Division

THALES

Low-level services:

- Hosted by a device
- Providing a « basic » function
- Monitored by SNMP/Syslog-NG/Web Services
- Characterized by a scope

High level services:

- A pure abstraction to describe the monitored system
- Depends on one or many low-level services
- Monitored by underlying performance/availability metrics composition
- Characterized by a scope

8 Land & Joint Division

THALES

Very often, one cannot manage the whole service chain: many actors operate to provide an end-to-end service. That fact is represented here by the “domain” concept: something that we are unable to directly act on, but with which we could negotiate and exchange some “SLS”

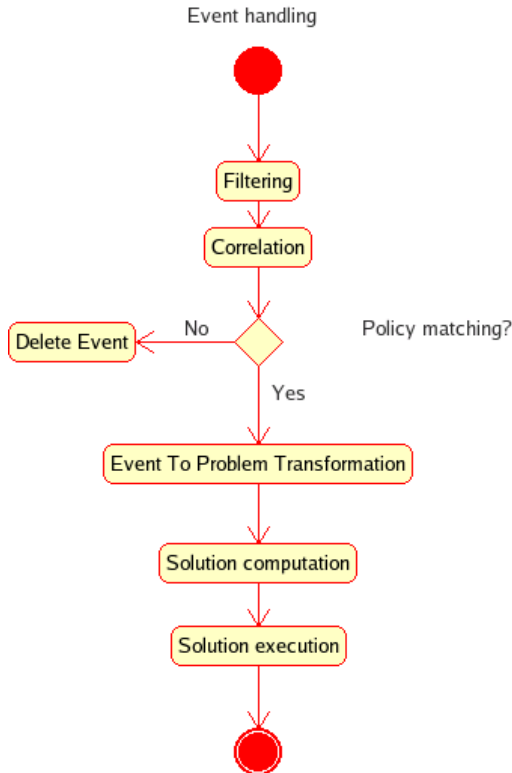


Services are built to monitor business oriented objectives

Graphs are automatically created for each service to represent its performance

This allow a better interpretation of network information into human manageable form and help to interpret high level management objectives





An event is received: Perf = 5

A policy has been set:

For this kind of service, if the perf < 6, find an improvement!

This event is converted into Problem:

We insert in the KB the fact: there is performance problem concerning such kind of service on this host.

The decision engine compute some solutions and propose a list to the operator

Intuitively, human correlate easily a **red flashing light** on their supervision console with the 200 incident tickets queuing...

But what for a machine?

We need to « explain » that an over passed threshold means a performance problem!



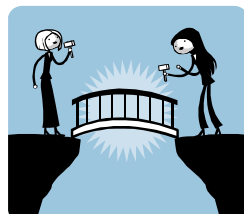
It consists in using models to **capture knowledge** relating to network capacities, environmental constraints, business objectives...

...together with ontological engineering to provide **inference capabilities**

An **ontology** is a data model that represents a set of concepts within a domain and the relationships between those concepts. It is used to reason about the objects within that domain.

Usually, a data model may have many ontologies: we use ontologies to represent relationships and semantics which cannot be represented using information language as UML.

How to describe: « is similar to », « is a kind of »



A typical Prolog program will form a knowledge base -- **a database of facts and rules** which is used as a basis for inferences. To initiate computations, you just query the knowledge base.

```
couldSolveProblemInSuchAScope(forceFreeUnusedChannels,  
    'IPTV').
```

```
couldSolveProblemInSuchAScope(InstallSecurityPatch, 'Sec  
couldSolveProblemInSuchAScope(StartApplication, 'AnyScope
```

Each line in this program asserts a fact.



Once the knowledge base populated, we can interrogate the Prolog system. I can **enter questions and receive answers.**

```
?-couldSolveProblemInSuchAScope(forceFreeUnusedChannels, 'IPTV').  
yes
```

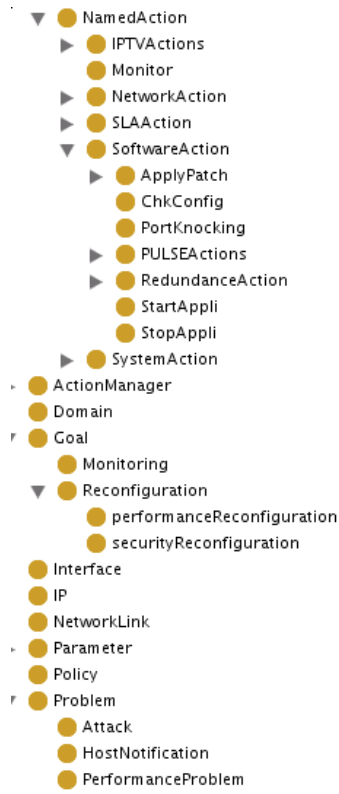
That means: "Could 'forcefreeunusedchannels' solve problems related to IPTV?"

Prolog says, "Sure does."

```
?-couldSolveProblemInSuchAScope(X, 'Security').  
X = 'InstallSecurityPatch'  
yes
```

Which means: "What are the available action to solve a problem related to security? Prolog found one solution in this knowledge base: install a security patch





Basic concepts (meanings)



To « understand » and to be able to react on changes, our system must at least understand what is:

- A **service**: and how is it linked with other services and/or with some physical devices? What is its **status**?
- A **problem**: what kind of problem? Security, performance...
- A **reconfiguration action**: which of them are available? where? How to use them? Which **impacts** on the system (that means from which state to which other one)?

The screenshot displays a software interface with two main panels. On the left is a hierarchical tree structure under the root 'owl:Thing'. The tree is expanded to show 'Action', which includes sub-categories like 'DiffusedAction', 'ManualAction', 'NamedAction', 'IPTVActions', 'Monitor', 'NetworkAction', 'SLAAction', 'SoftwareAction', 'PULSEActions', 'RedundanceAction', and 'SystemAction'. The 'DownloadSecurityUpdate' action under 'PULSEActions' is highlighted. On the right is a 'Property' view for 'rdfs:comment' with the value 'Ask to PULSE server to download a iven security update'. Below this, there are several expandable items, including 'PULSEActions' with various properties like 'coutGene has 10', 'coutRisqueSecureite has 10', and 'hasPrecondition some not Blocked'. The 'CheckSecurityUpdateMatch' action is also visible at the bottom of the right panel.

Semantic annotations to capture the knowledge



To link the real world with this model, semantic annotations are used on real instances of previously modelled concepts.

For instance a process running on a Linux host could be annotated as a « DB process ».

Thus, the system knows more than its pid only:

It knows what kind of actions could be considered if a problem impact this process, and which impacts on the linked services

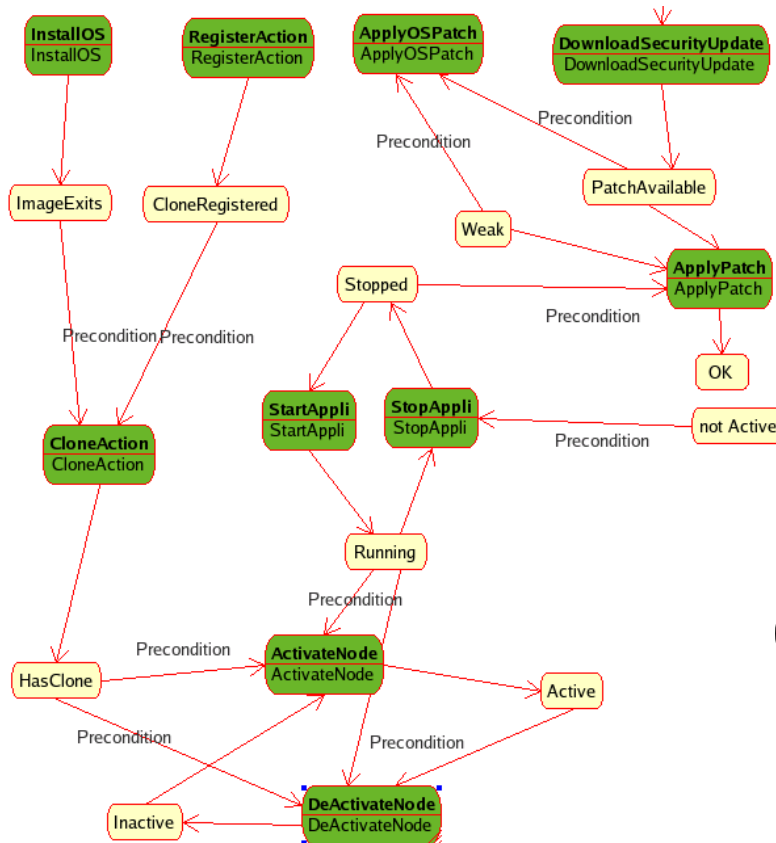
```

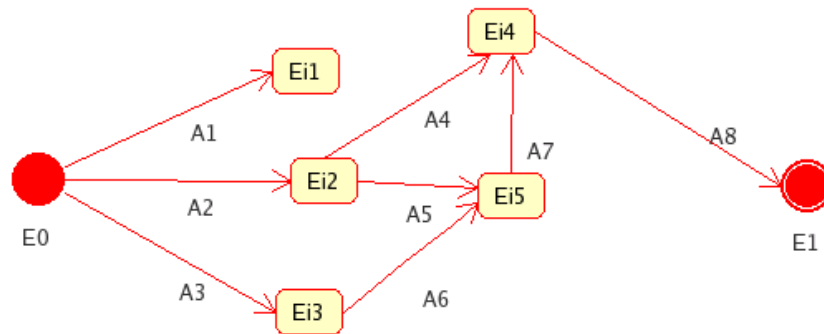
xmlns:sawsdl="http://www.w3.org/2002/ws/sawsdl/spec/sawsdl#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:tns="http://www.thales.com/tai/Energy">

<wsdl:types>
  <xsd:schema targetNamespace="http://www.thales.com/tai/Energy"
    xmlns:sawsdl="http://www.w3.org/2002/ws/sawsdl/spec/sawsdl#"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified">
    <xsd:complexType name="AscendingRequest">
      <xsd:sequence>
        <xsd:element type="xsd:string" name="param"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="AscendingResponse">
      <xsd:sequence>
        <xsd:element type="xsd:int" name="param"
sawsdl:modelReference="http://www.thales.com/energy.owl#Performance"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="DescendingRequest">
      <xsd:sequence>
        <xsd:element type="xsd:string" name="param"/>

```

The Status Graph (cf)





Ai: Atomic actions

{A2, A4, A8}: global reconfiguration solution

Solutions are ranked, according to relevant metrics
(number of actions, vulnerability, security, availability...)

A solutions' list is presented to an operator
The chosen one is executed on the managed system

Different **actuators** are available:

- Semantically augmented Web Services
- Service Level Specification exchange
- Semantically augmented Netconf requests

Providing that a semantic description is possible, any legacy equipment, software could be seen as effector or actuator

Domain experts must however explain how to use this equipment, if there are some preconditions and what are the impacts on the monitored systems: they have to store their knowledge into an ontology



Possibility to deploy a hierarchy of management console (supervision) to provide consolidated views of network and system availability (hypervision).

It remains a real issue for very large and complex systems

Provide a business view of the managed Information System

Decrease the down-time

Is more reliable, avoiding natural human error

Allow an iterative design loop to adapt the tools to any IS changes or technological important steps.



Thank you for your attention



<http://itea-energy.eu>
Have on look!