Christophe Chareton, Julien Brunel, David Chemouil

REQUIREMENTS ENGINEERING AND MULTI-AGENT TEMPORAL LOGIC

WORK IN PROGRESS

2011-01 IFIP WG 1.3 meeting, Aussois

CONTEXT

- Aim: to provide "pragmatic" foundations to formalize parts of requirements engineering (RE) techniques.
- Our approach may be situated at the intersection of RE and logic, from the model-checking community's point of view. This presentation is based upon a forthcoming submission to a conference in the RE community.

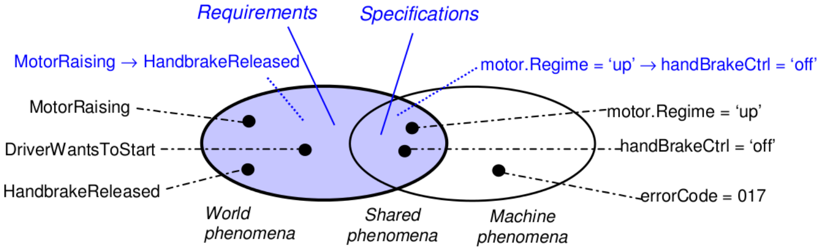
RE (WITH A NARROW VIEW)

- For decades, industry polls have showed that for around 60% of partly or totally failed software projects, *requirements* were spotted as the main reason for failure.
- RE is concerned with eliciting, analysing, expressing, capitalizing, maintaining, evolving, etc., customers' requirements.
- Informally, a requirement is a non-ambiguous, understandable, precise, exhaustive, etc., statement that will have to be implemented in the system to be, and that can be directly traced and justified wrt customers's needs or external constraints (laws, regulations, laws of nature...). (And more formally? see later.)

FORMAL VS INFORMAL

- A pragmatic definition of RE: a set of techniques, languages, heuristics, etc. that help perform the transition from an informal statement of needs to a formal specification.
  - A rule of thumb: if you are able to formalize a statement right from the beginning, you already have glossed over 90% of RE...
- So most of RE is concerned with writing a good specification, where "good" means understandable, justifiable, non-ambiguous, etc.
  - "Good" as nicely structured, amenable to verification, to generalization, refinement, etc. is more a question of *formal specification* (CASL, B, TLA...).
  - However, it is sensible to expect the outcome of RE to be formal, so the intersection between RE and formal specification is certainly not empty in practice.

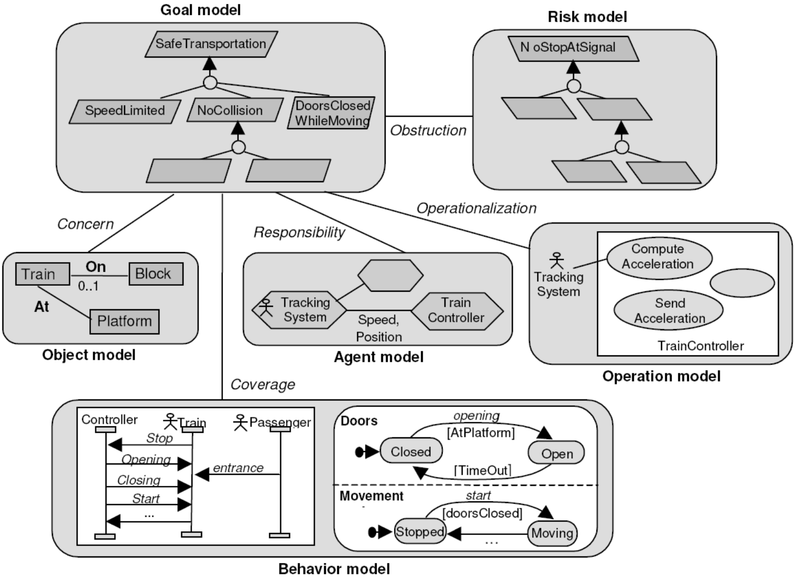
A BASIC ONTOLOGY



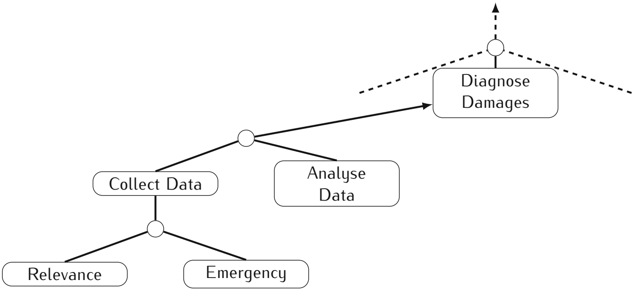
(Van Lamsweerde; Jackson, Zave & Gunter)

$$W, S \models R$$

THE KAOS FRAMEWORK



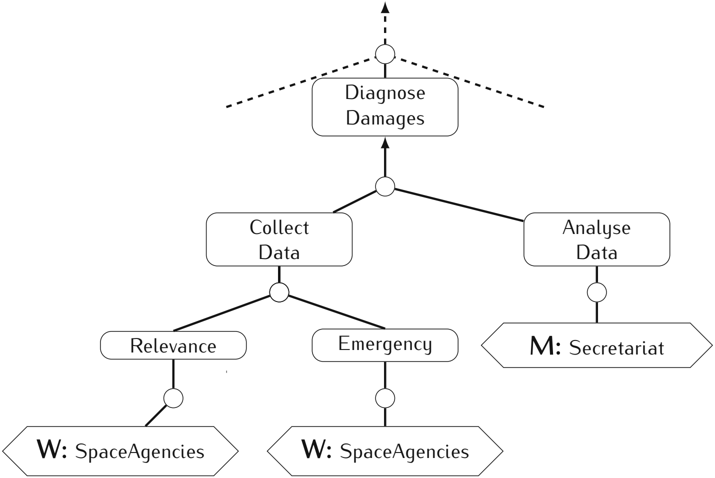
THE GOAL MODEL



$$\mathit{CollectData}, \mathit{AnalyseData} \models \mathit{DiagnoseDamages}$$

(formulae written in a first-order LTL with past operators)

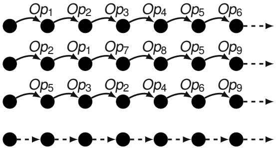
AGENTS, REQUIREMENT AND EXPECTATIONS



No semantic status for agents.

FROM GOALS TO OPERATION SPECIFICATIONS

From LTL to Floyd-Hoare...



Op	GetPictures
DomPre	NoPictureAvailable
DomPost	PicturesAvailable
ReqPost for **Usefulness**	Picture.time = 12.01.2010
ReqPost for **Usefulness**	Picture.place = haiti
ReqTrig for **Emergency**	Disaster

MEANING OF OPERATIONS

- $[\![Op]\!] := \textbf{DomPre} \wedge \textbf{XDomPost}$
- and we must have:
  - $[\![Op]\!] \implies \textbf{ReqPre}$
  - $[\![Op]\!] \implies \textbf{XReqPost}$
  - $\textbf{DomPre} \wedge \textbf{ReqTrig} \implies [\![Op]\!]$

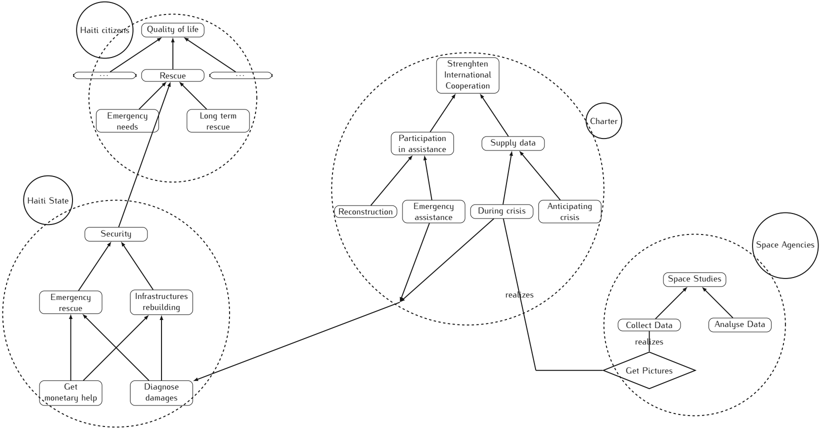
Then a requirement R is *operationalized* by operations $\{Op_i\}_{i \in I}$ if $\{Op_i\}_{i \in I} \models R$.

INTENTIONALITY OF THE AGENTS

TROPOS and i* (Mylopoulos, Yu, ...) insist more on early RE. The formal aspects are rather limited (propositional logic).

- A double relation agents-goals :
  - What agents are in charge of, what they realize (KAOS sense)
  - What they aim for, what they wish
- Interests :
  - Guide the assignement
  - Answer the *why* questions
  - Exhibit dependencies
  - Integrate human or institutionnal agents : a social dimension

INTENTIONALITY OF THE AGENTS



USING PRE-EXISTING AGENTS

- Pre-existing agents can be used so as to ensure a part of the goal model
- An actual means for confronting agents and their capabilities with what is expected from them.

CONCLUSION

	KAOS	TROPOS
Rigorous need analysis	×	
Relation goal-operation	×	
Temporal semantics	×	
Intentional agents		×
Means-ends analysis		×
Assignements decision		×
Multi-agents semantics		

AIMS

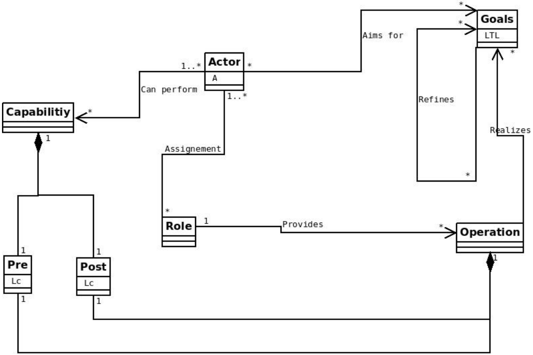
- Integrate the agents' intentions and means-end analysis …
  - Agents pursued goals
  - Agents ability to adopt roles from the goal analysis

  …in a structured language inspired by KAOS
- Give a semantics that takes into account time and agents, using ATL in this presentation

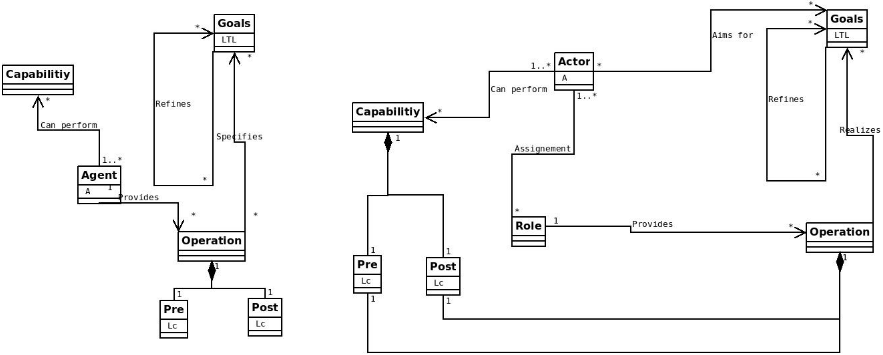
METAMODEL

- A **capability** is a pair of conditions (pre, post)
- **Actors** and **roles** are respectively specified through **capabilities** and **contracts**, which share a common language : they are possible values for a set of state variables.
- **Actors** have a double relation with

  goals :
  - The direct **Aims for**, as actors.
  - The realization, through requirement and specification, via the roles they are assigned to.



METAMODEL : COMPARISION WITH KAOS



CAPABILITIES

X is a finite set of variables :

$$X = \{x_i\}_{i \in Ifinite}$$

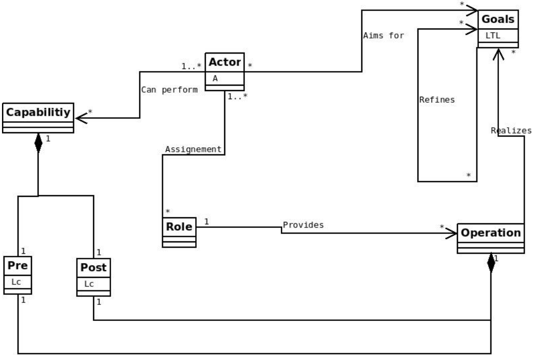
- $\mathcal{L}_C$ is given by the following grammar :

  $$\varphi ::= x \sim n \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg \varphi$$

  where :
  - $x \in X$
  - $n \in \mathbb{N}$
  - $\sim \in \{, >, = \leq, \geq\}$
- LTL is given by the following grammar :

  $$\varphi := p \mid \neg \varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathbf{X}\varphi \mid \varphi \mathbf{U} \varphi$$

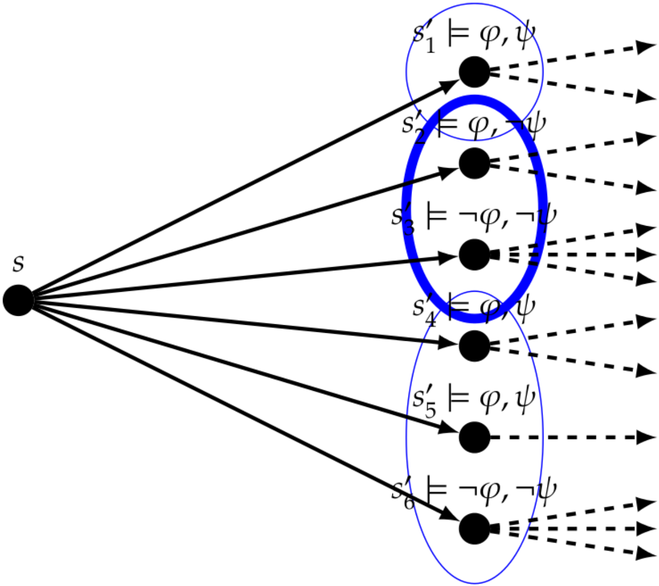
  where $p \in \mathcal{L}_C$



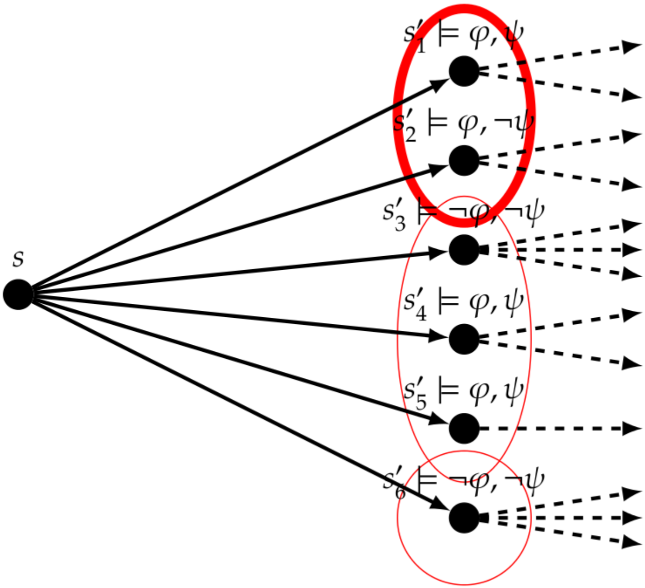
A CRASH COURSE ON ATL

ATL (Alur, Henzinger, Kupferman) is an extension of CTL that introduces agents and coalitions of agents. So it contains tool to express such things as: agent x or the group of agents A is able to ensure φ.

$$p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \langle\langle A \rangle\rangle \mathbf{X}\varphi \mid \langle\langle A \rangle\rangle \varphi_1 \mathbf{U} \varphi_2$$



$$M, s \models \langle\!\langle A_1 \rangle\!\rangle X \neg\psi$$



$$M, s \models \langle\langle A_2 \rangle\rangle X \varphi$$

LANGUAGE

- $[\![A.canPerform]\!] := \bigwedge_{cap \in A.canPerform}(cap.pre \rightarrow \langle\!\langle A \rangle\!\rangle \mathbf{X} cap.post)$
- $[\![refines(\{G_i\}_{i \in J}, G)]\!] := \{[\![G_i]\!]\}_{i \in J} \models [\![G]\!]$
- $[\![realizes(\{op\}_{i \in J}, G)]\!] := \{\Box(op_i.pre \rightarrow \mathbf{X} op_i.post)\}_{i \in J} \models [\![G]\!]$
- $[\![aRole]\!] := \bigwedge_{op \in aRole.provides} \Box(op.pre \rightarrow \mathbf{X} op.post)$

DERIVED RELATIONS

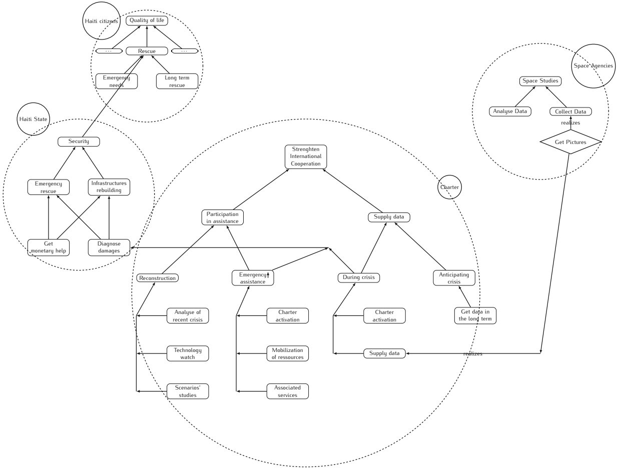
- We note $\mathit{Adequation}(\mathit{aRole}, A)$ iff from A's capability we can derive that it is able to play role aRole:

$$[\![A.\mathit{canPerform}]\!] \models \langle\!\langle A \rangle\!\rangle [\![\mathit{aRole}]\!]$$

- We note $\mathit{Adequate}(\mathit{assig})$ iff each role aRole in Roles is assigned to an adequate actor, iff :

$$\bigwedge_{\mathit{aRole} \in \mathit{Roles}} \; \bigwedge_{A \in \mathit{aRole}.\mathit{assig}} \mathit{Adequation}(\mathit{aRole}, A)$$

GOAL DIAGRAM FOR THE CHARTER



ROLES

- Emergency assistance :
  - Charter activation :
    - (BeneficiaryBody, Disaster, RequestIntervention)
    - (Secretariat, RequestIntervention, ConfirmRequest)
  - Mobilization of ressources
    - (Party, CrisisSituation, PlanAvailabiityOfSpaceFacilities)
  - Associated services
    - (Party, Disaster, AssociatedServices)
- Supply data during crisis :
  - Charter activation
  - Supply data
    - (Party, Disaster $\wedge$ NoPictureAvailable, Available.Pictures $\wedge$ Pct.time = disaster.t $\wedge$ Pct.place = disaster.p))

ASSIGNEMENT *assig*

- Beneficiary Bodies → Haiti State
- Parties → *Agencies and Space Systems*:
  - European Space Agency (ESA)
  - Centre national d'etudes spatiales (CNES)
  - Spotimage
  - NSPO
  - Canadian Space Agency (CSA)
  - Indian Space Research Organisation(ISRO)
  - National Oceanic and Atmospheric Administration (NOAA)
  - Argentina's Comision Nacional de Actividades Espaciales (CONAE)
  - Japan Aerospace Exploration Agency (JAXA)
  - United States Geological Survey (USGS)
  - Digital Globe
  - **GeoEye**
  - DMC International Imaging (DMC)
  - Centre National des Techniques Spatiales (Algeria)
  - National Space Research and Development (Nigeria)
  - Tabitak-BILTEN (Turkey)
  - BNSC/Surrey Satellite Technology Limited (UK)
  - BNSC/Qinetiq (UK)
  - China National Space Administration (CNSA)
- Secretariat → *Secretariat*

TACKLED PROBLEMS :

- Checking assignement : decide whether an assignement *assig* is adequate either for the whole model or for a subpart of it (induced by a subset of roles or a subset of goals)
- Existence of an assignement : decide whether there is an assignement that is adequate for either the whole model or a subpart of it, and if yes give one.

ACHIEVEMENTS

- The goal-decomposition structure inherited from KAOS
- A specification of the operations to satisfy the goals
- Distributed intentionality inherited from $i*$
- Means-end analysis and a double concept of provided-required agent (actor vs role)
- A multi-agent semantics

FURTHER ENRICHMENTS

- Introduce a concept of effective behaviour in the semantics (ATL with context, $Strategy - ATL$ ...). Hence :
  - Distinguish agents' possible behaviour from their effective behaviour
  - Means for comparing different behaviour in efficiency towards goal's satisfaction, mutual coherence
- Meta-theoretical properties of the logic (model-checking, satisfaction, complexity)
- Links with architecture models