



Escola Politécnica da USP

PMR 5020

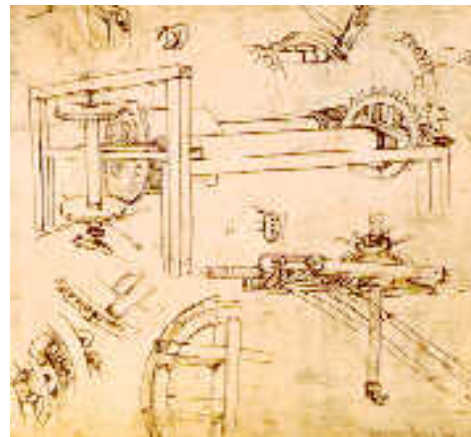
Metodologia do *Projeto* de Sistemas

Aula 6: Especificações



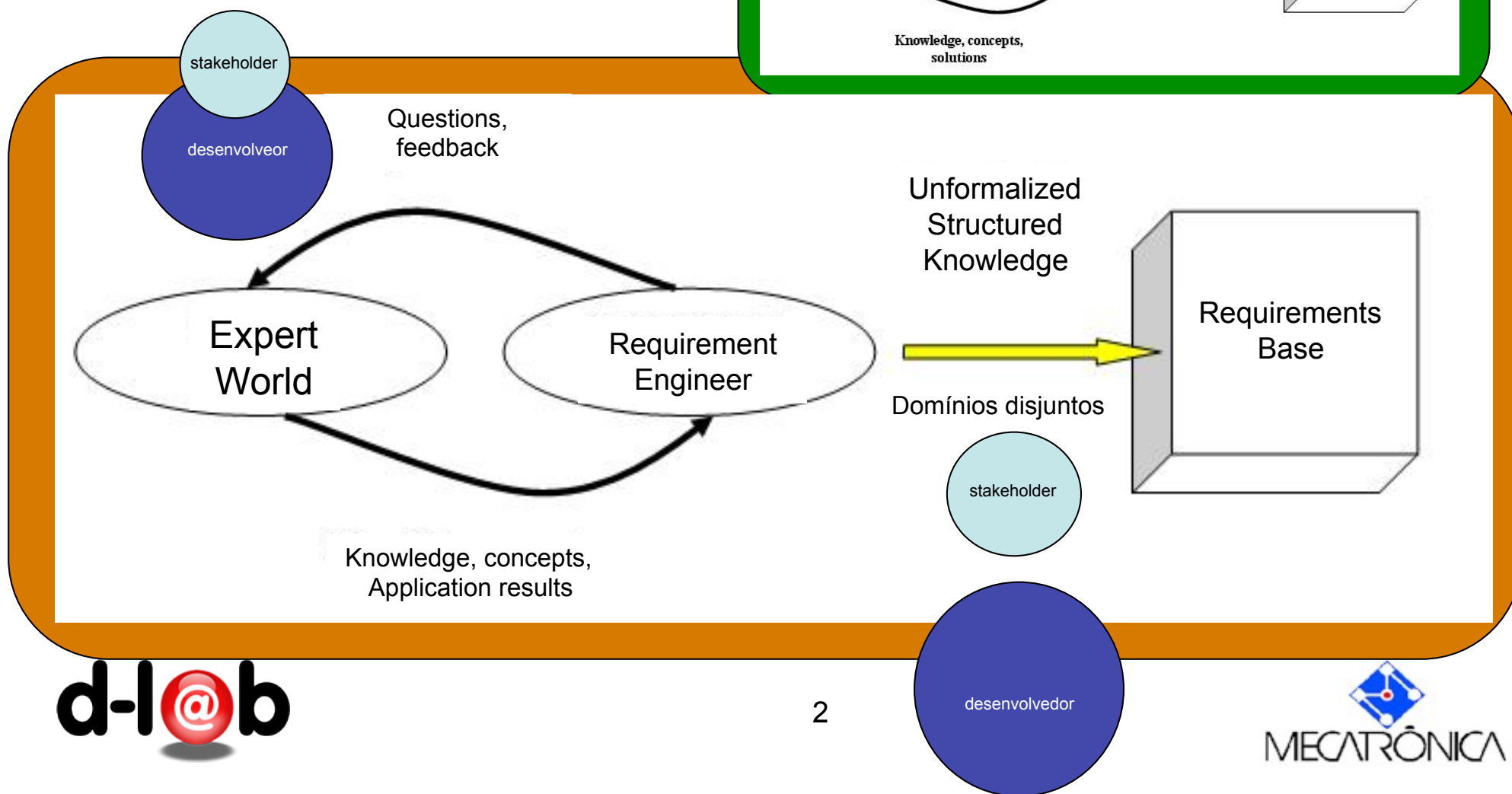
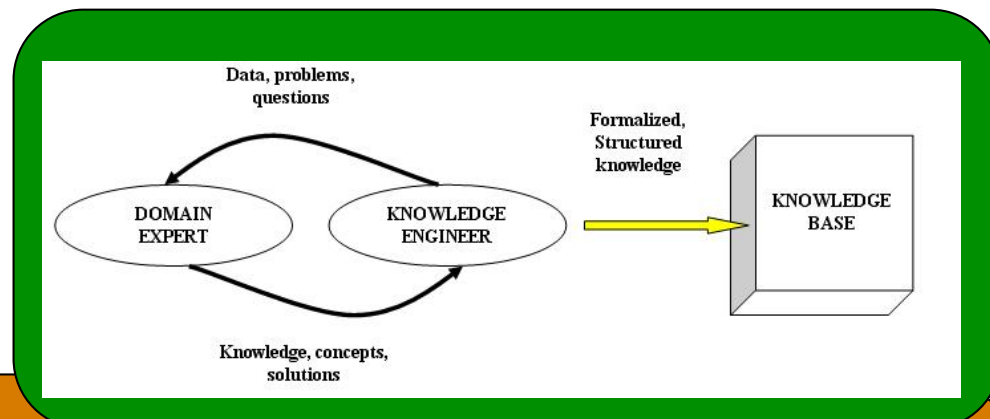
Prof. Dr. José Reinaldo Silva

reinaldo@poli.usp.br





O Processo de eliciação





Knowledge Engineering



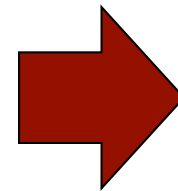
Edward Feigenbaum
“Pai” dos Sistemas Especialistas
Stanford University

KE is an engineering discipline that involves integrating knowledge into computer systems in order to solve complex problems normally requiring a high level of human expertise



Knowledge Engineering

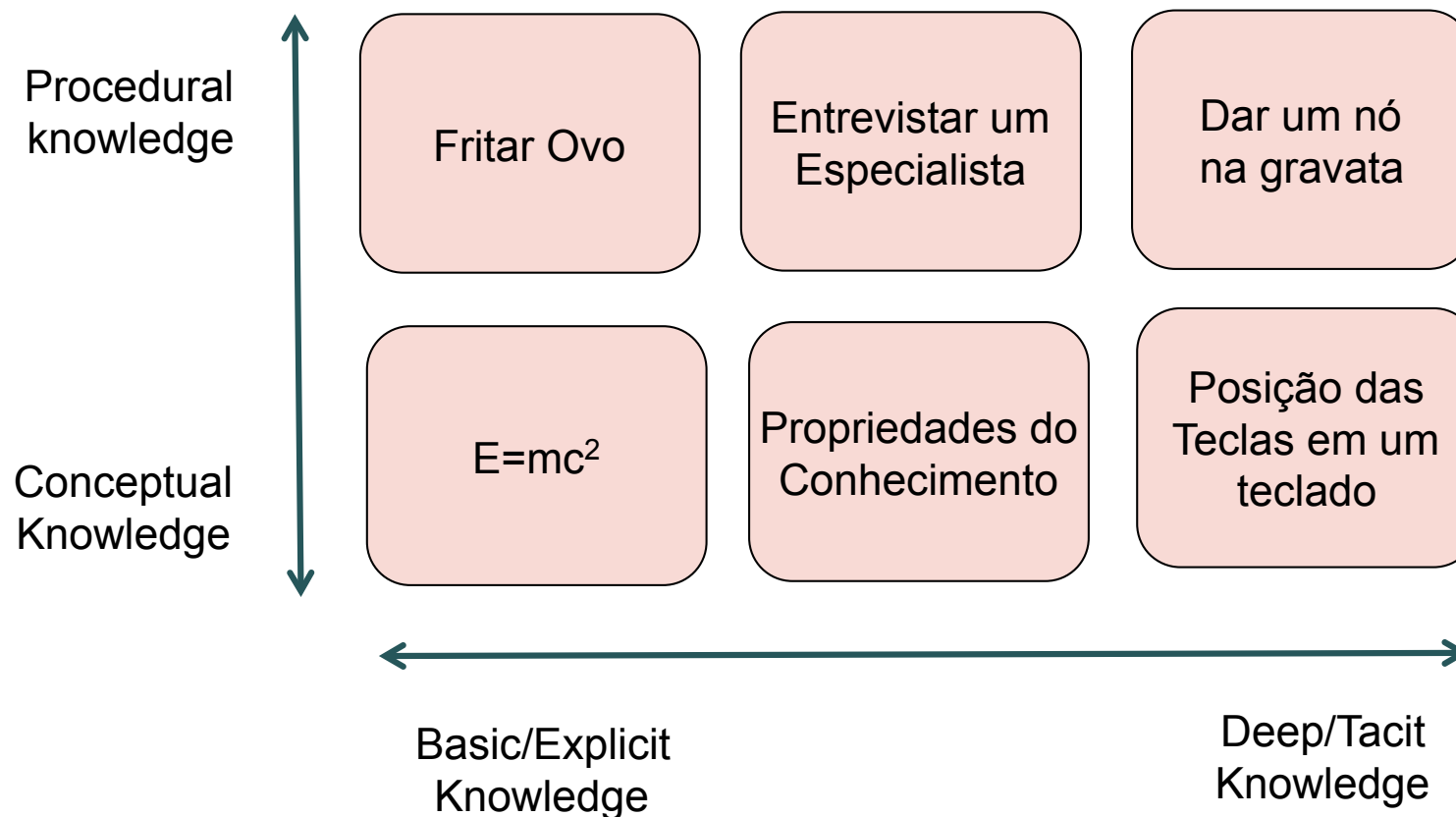
Knowledge Acquisition
Knowledge Modeling and Analysis
Knowledge Validation
Knowledge Base Building



**KNOWLEDGE
ENGINEERING**

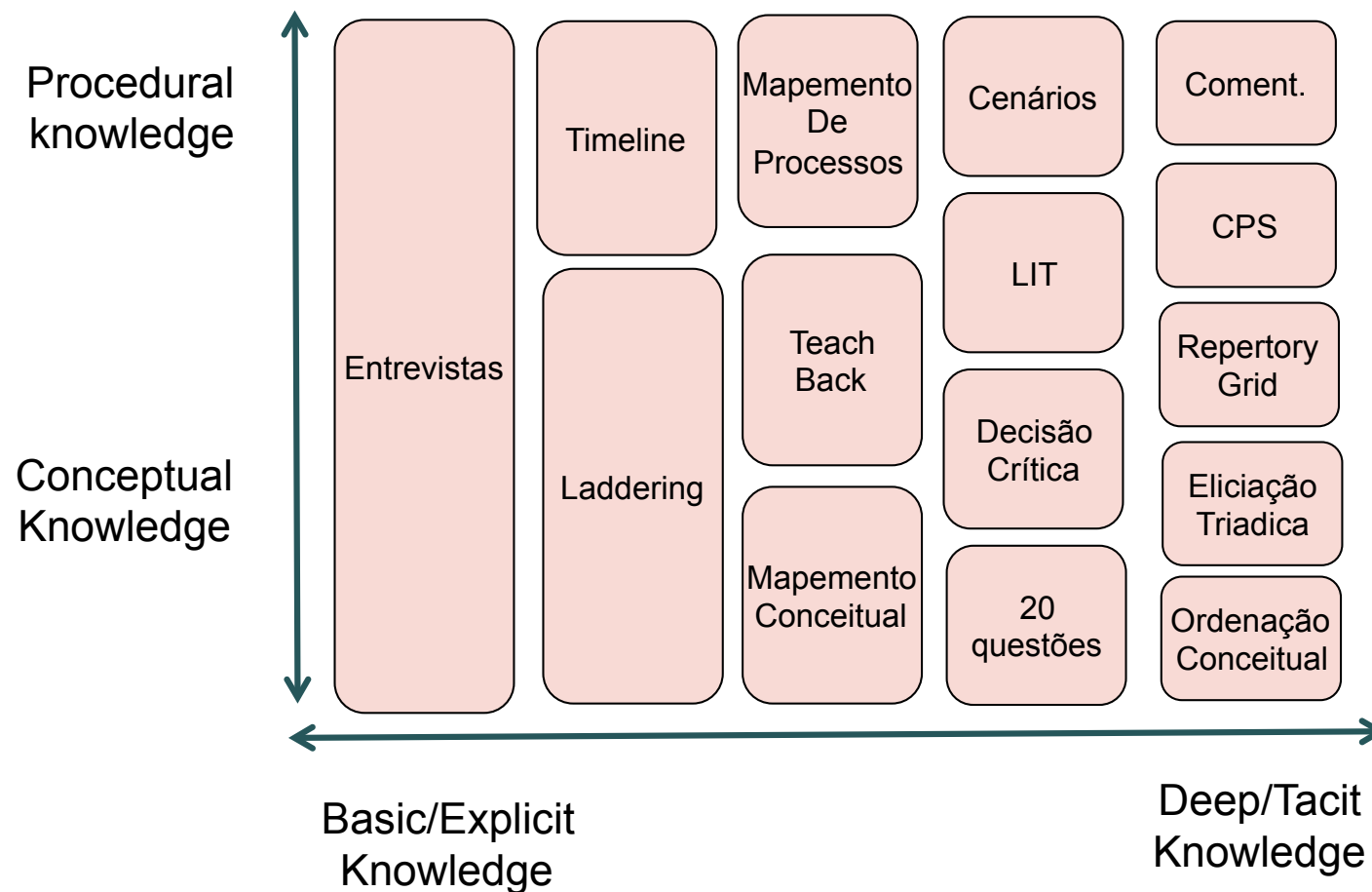


Knowledge Types





Knowledge Elicitation





Técnicas de Eliciação

Técnicas Tradicionais

- Introspecção
- Pesquisar documentos existentes
 - Entrevistas
 - Abertas
 - Fechadas
- Questionários
- Reuniões

Técnicas Colaborativas

- Técnicas de grupo
 - grupos temáticos
 - brainstorming
- JAD/RAD workshops
- Design participativo

Técnicas Cognitivas

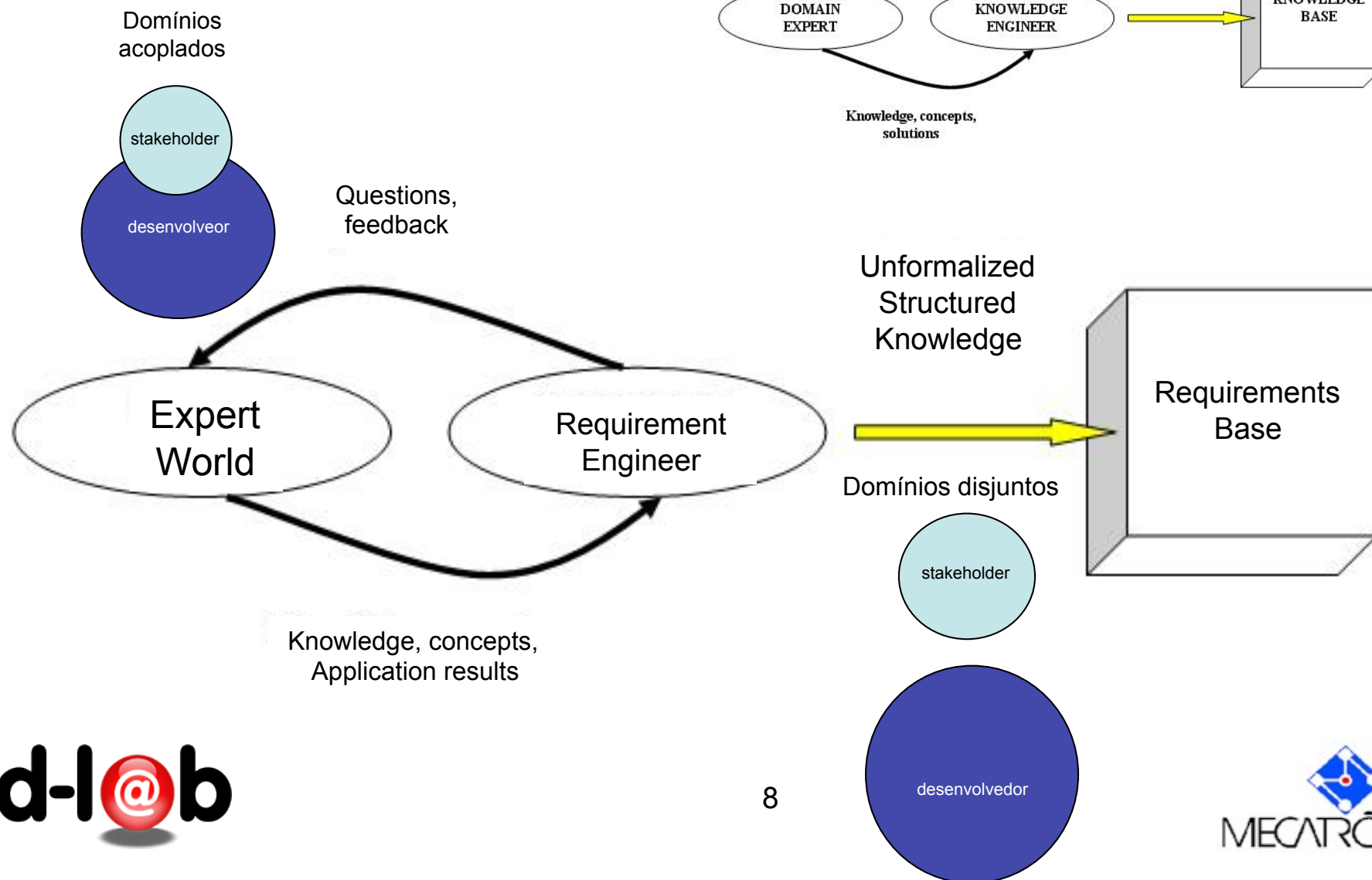
- Task Analysis
- Análise de protocolo
- Aquisição de conhecimento
 - Card sorting
 - Laddering
 - Repertory Grids
 - Proximity Scaling Tech

Abordagens Contextuais

- Técnica Etnográfica
 - Observação participativa
 - Etnometodologia
- Análise do discurso
 - Análise de intenções
 - Speech Acts
- Método Sociotécnico



O Processo de eliciação



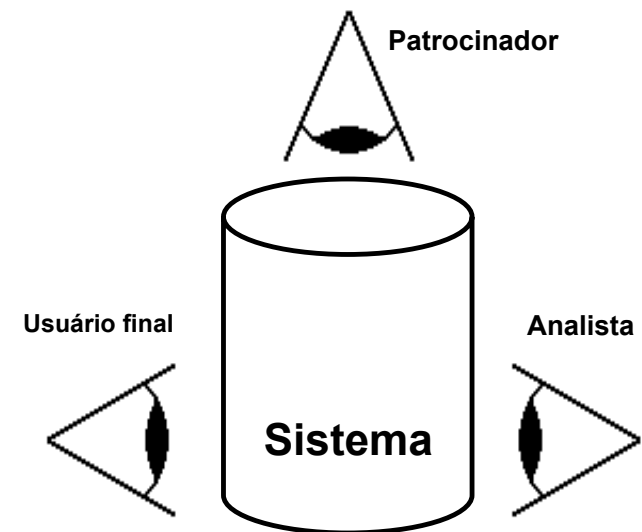


O Ciclo da ER

Refinando o ciclo de vida da ER, temos as seguintes fases:

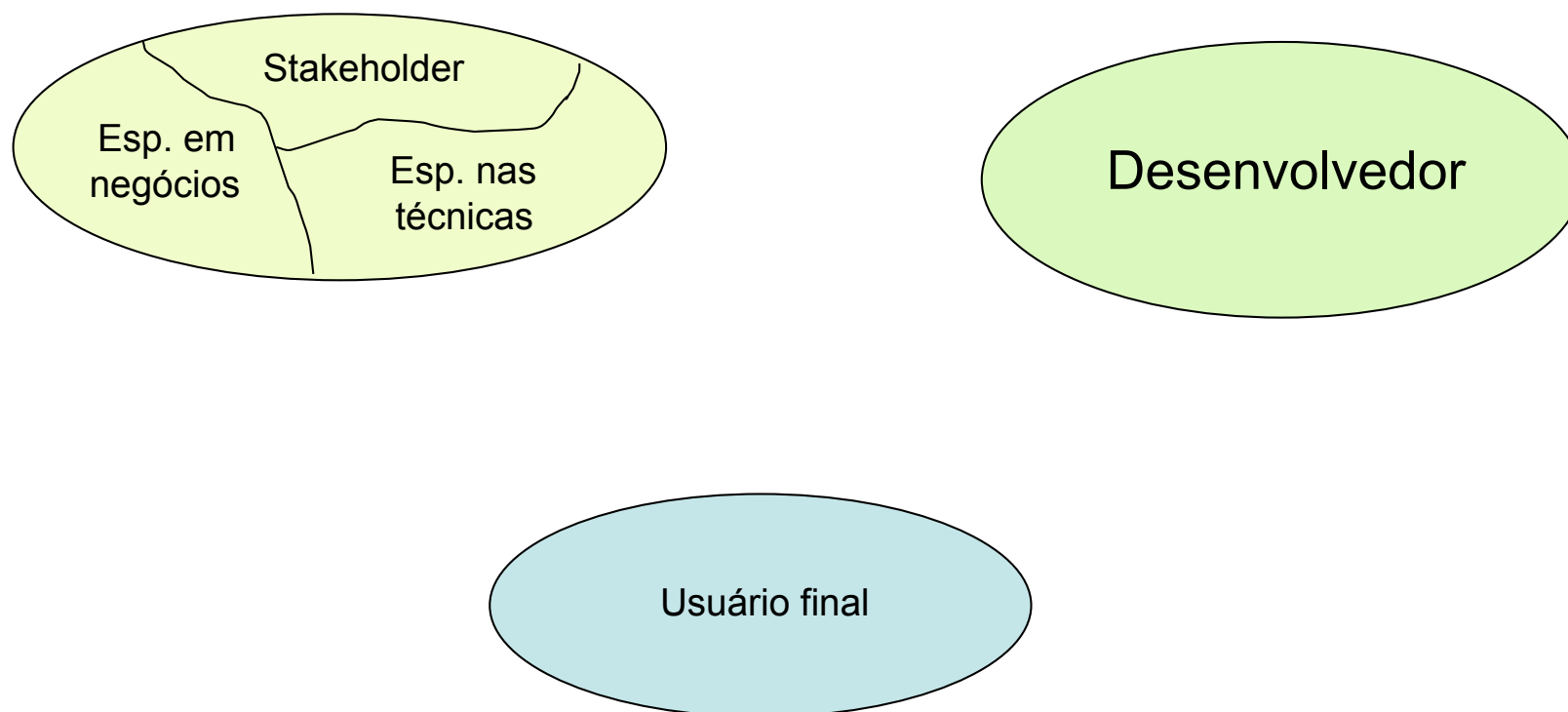
- Síntese do problema
- Eliciação de requisitos
- Análise de Requisitos
- Especificação de requisitos
- Verificação e validação
- Gerenciamento de requisitos

{ Modelagem
Análise
Validação local



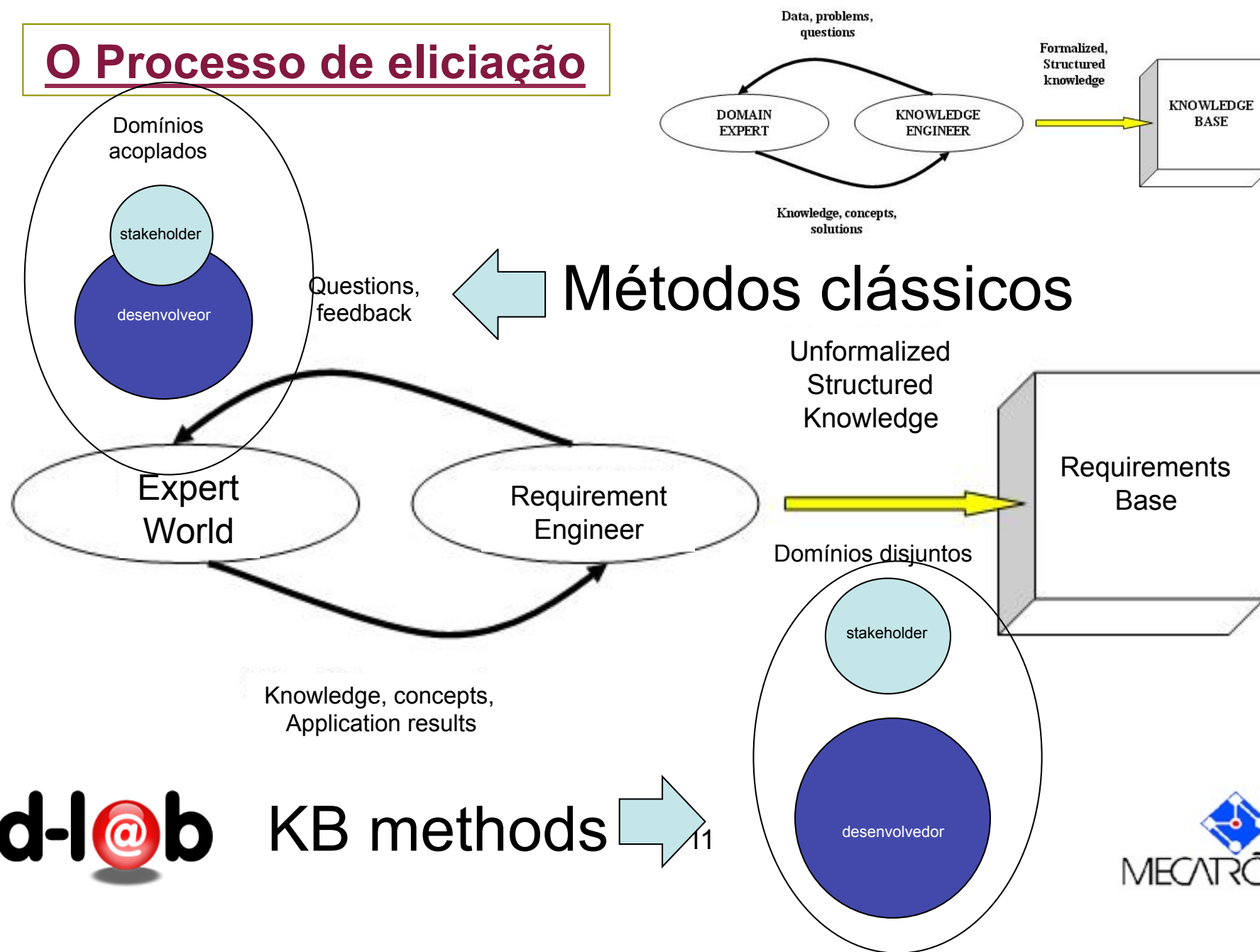


Distância entre domínios





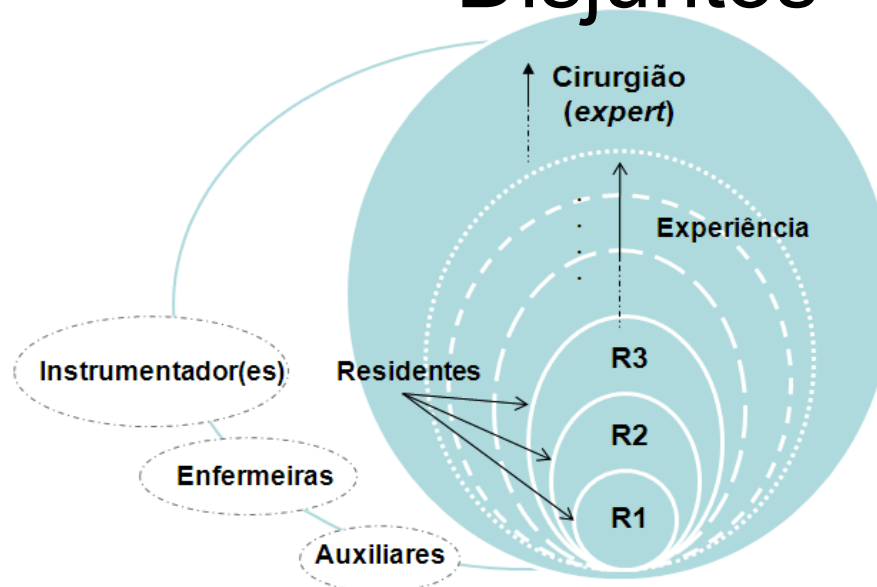
O Processo de eliciação

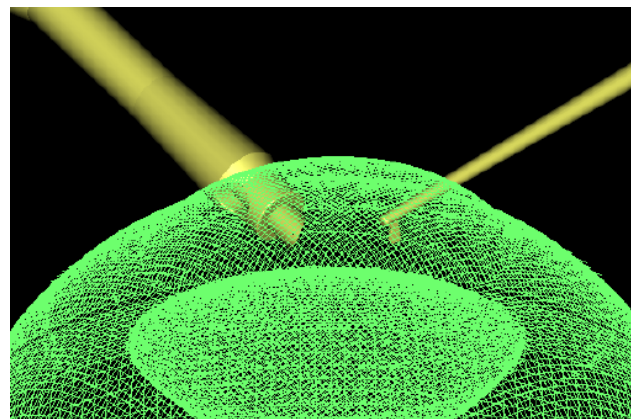
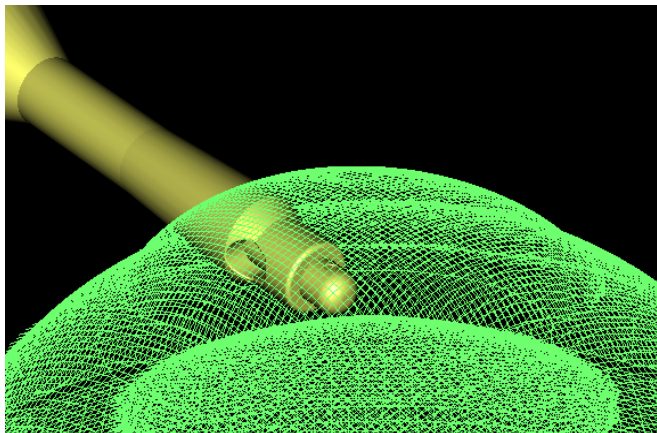
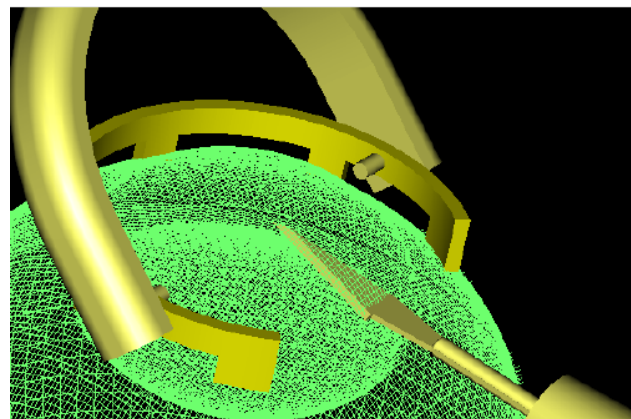
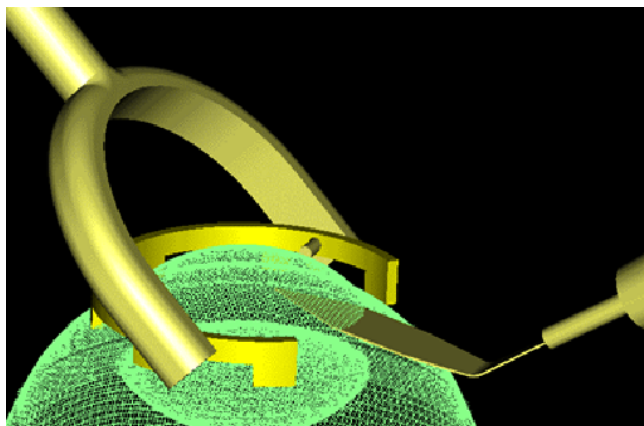




Domínio da Engenharia

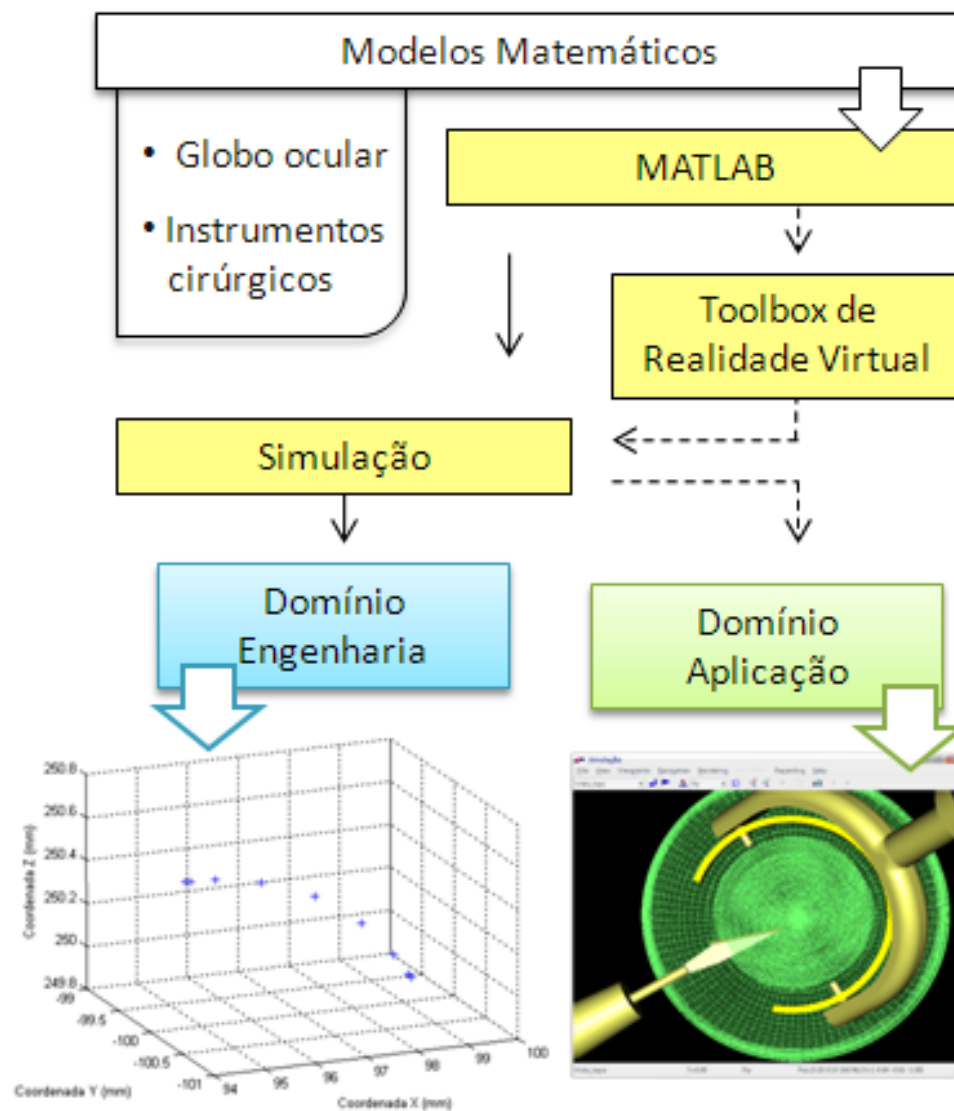
Domínios Disjuntos







Queiroz, R.A.A., and Silva, J.R.; Eliciação e Comunicação de Requisitos em Domínios Disjuntos: Estudo de Caso para a Área Médica, submetido à revista Controle e Automação, Sociedade Brasileira de Automação.





Resumo

Neste trabalho temos uma experiência com:

Eliciação pelo método etnográfico, com inserção do observador;

Extração de requisitos de sistemas complexos em um domínio disjunto;

Vivência do problema de “formalização” destes requisitos;

Tratamento do problema da comunicação e validação com o stakeholder através de prototipação rápida feita em MatLab e com visualização do potencial artefato.



Eliciação e comunicação de requisitos em domínios disjuntos:
estudo de caso para automação na área médica

Requirements elicitation and communication in disjoint
domains: case study in automation to surgical processes

Ricardo Alexandre de A. Queiroz; José Reinaldo Silva

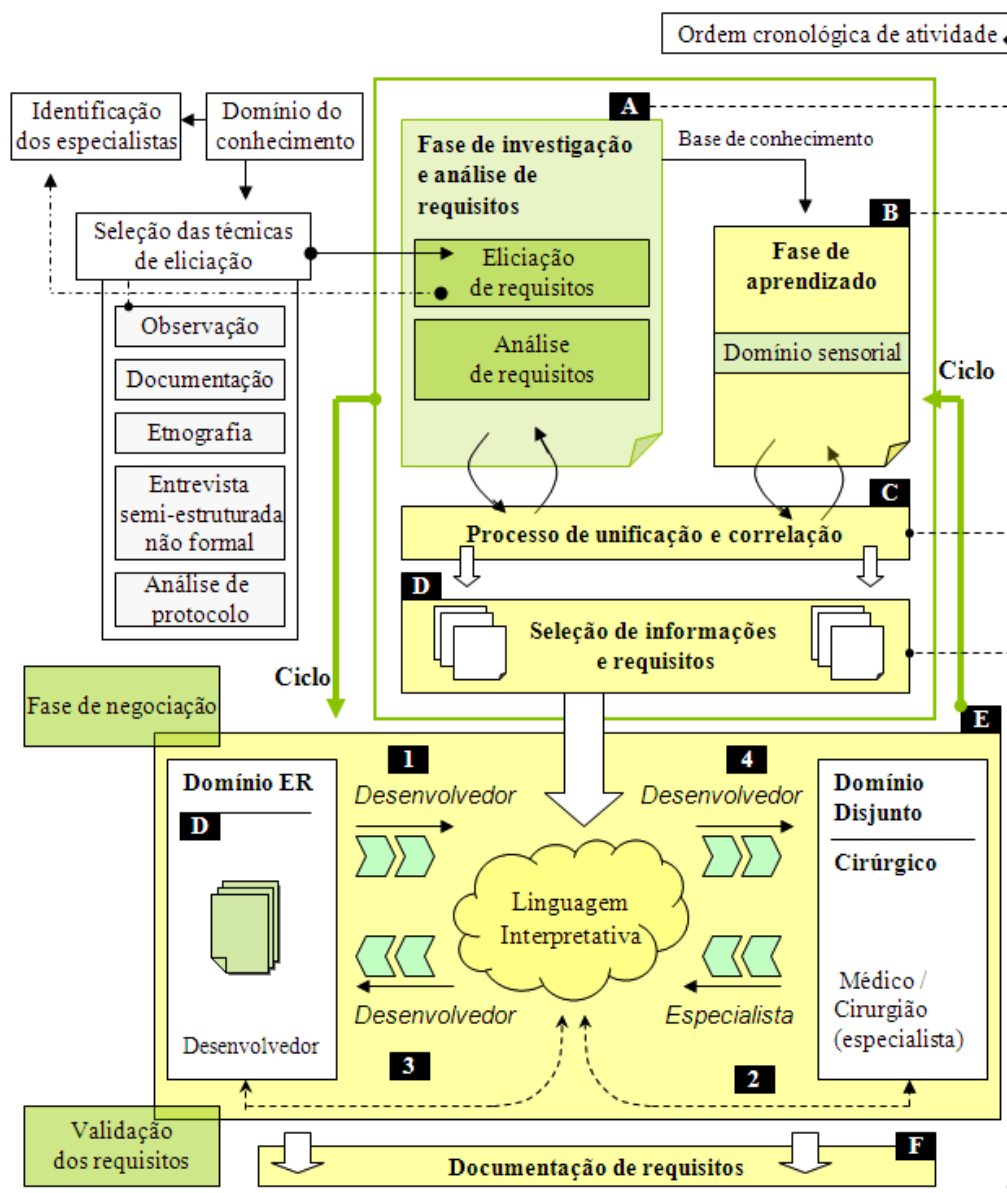
Revista: Controle & Automação Sociedade Brasileira de Automatica

Print version ISSN 0103-1759

Sba Controle & Automação vol.20 no.4 Natal Oct./Dec. 2009

doi: 10.1590/S0103-17592009000400014

Um exemplo: domínios disjuntos





Classificação dos métodos de análise

Os métodos de análise podem ser classificados como:

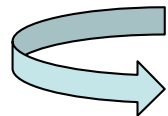
1. Análise dinâmica (animação);

2. Métodos baseados em conhecimento

Case based reasoning (CBR)
Constraint Satisfaction
KBS analysis and critics

3. Análise de consistência

Verification
Model checking



Validação

P
R
O
T
O
T
Y
P
I
N
G



Traceability ?





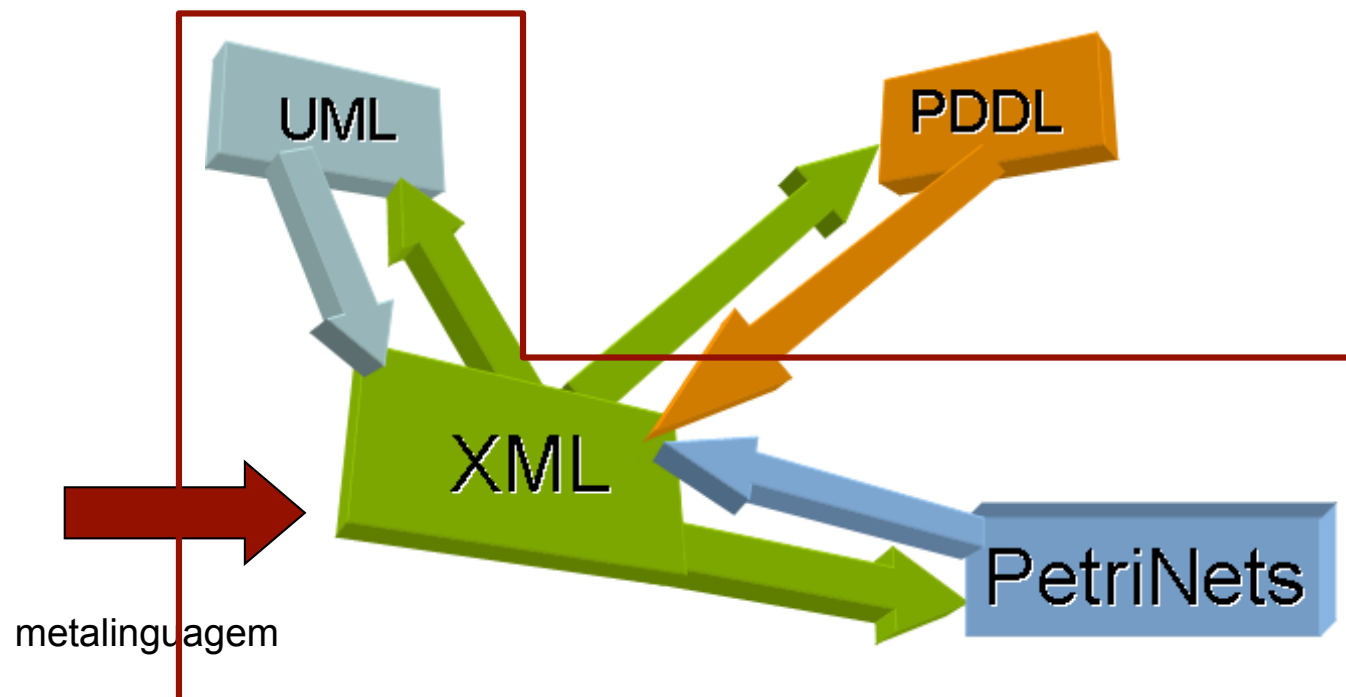
The traceability concept

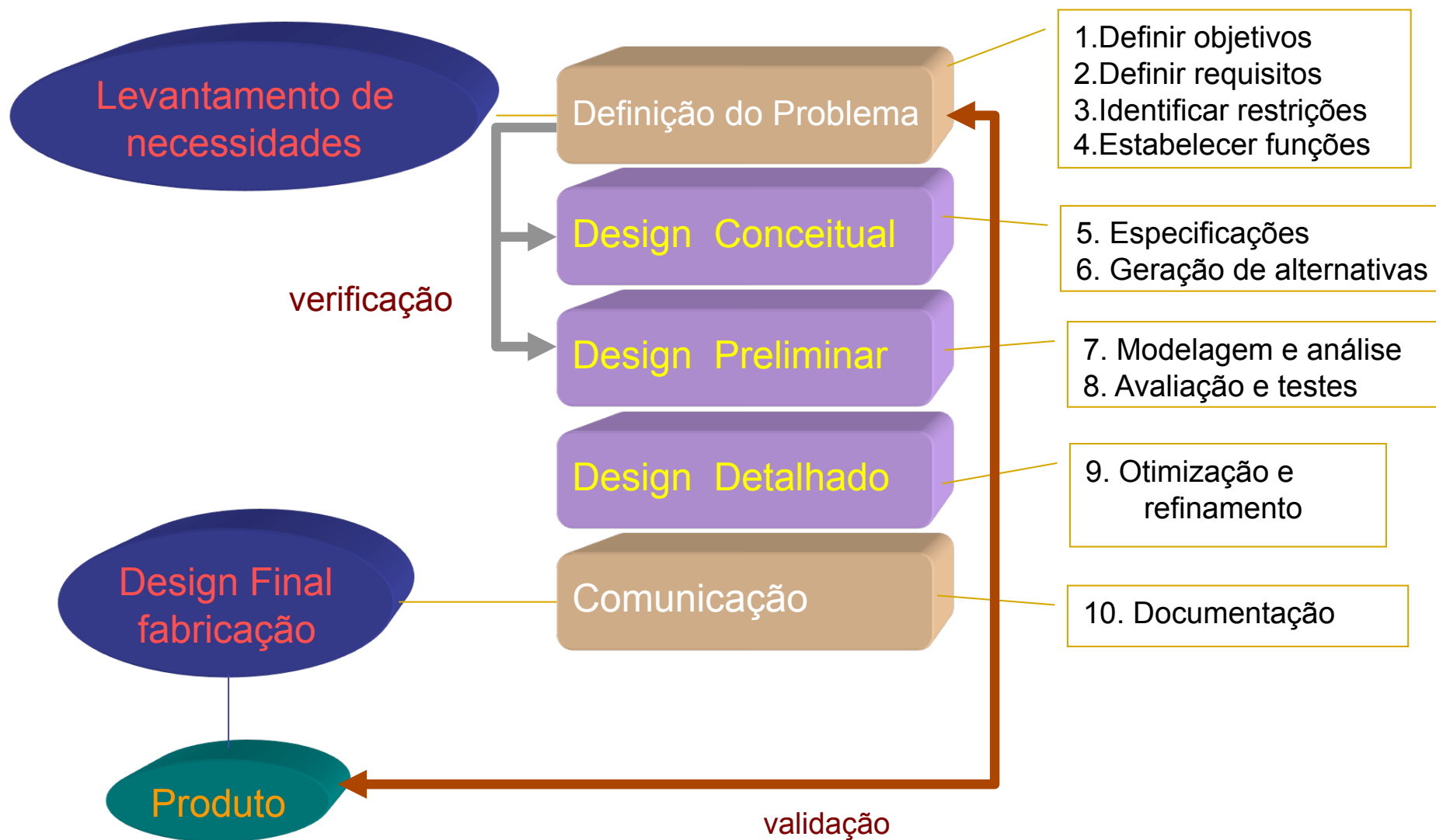
- Traceability is concerned with the relationships between requirements, their sources and the system design
- Source traceability
 - Links from requirements to stakeholders who proposed these requirements;
- Requirements traceability
 - Links between dependent requirements;
- Design traceability
 - Links from the requirements to the design;



itSIMPLE

Linguagem para especificação de planos







Mecanismos de verificação

“... uma especificação de software é um contrato entre o especificador e o implementador definindo o sistema a ser construído. Portanto deve ser entendido de forma clara e sem ambiguidades por ambas as partes. Deste modo a transparência é o primeiro critério para julgar especificações.

Robert Balzer

Uma linguagem de especificação é tanto mais apropriada para uma dada área ou setor da Engenharia quanto mais fácil seja os mecanismos de verificação entre especificação e implementação, o que remonta ao formalismo utilizado e à disciplina de projeto imposta.



Modelo geral

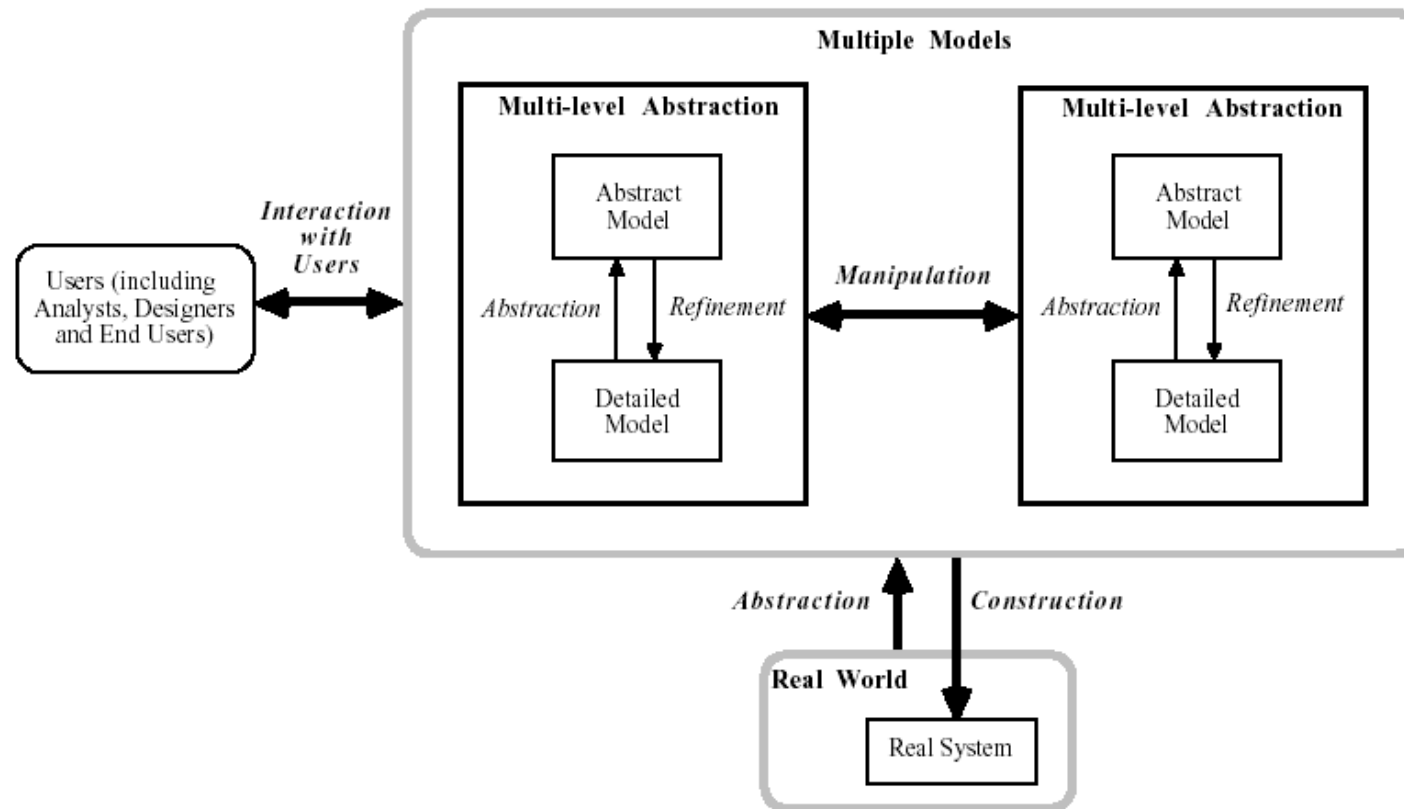
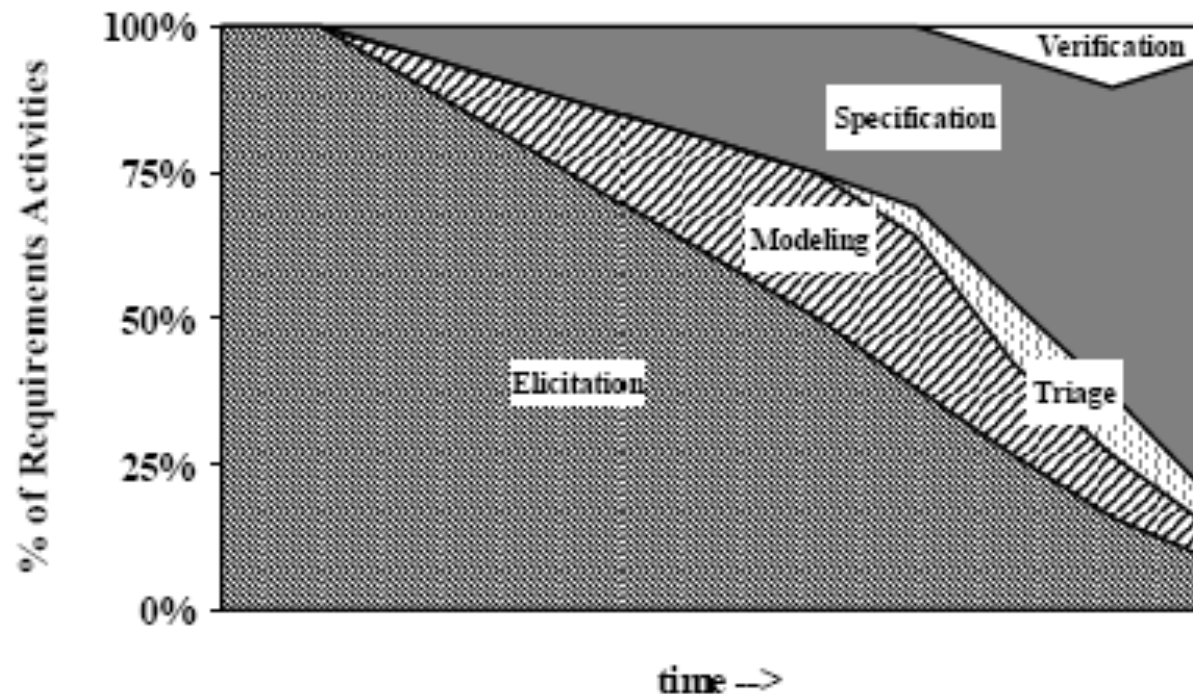


Figure 1 Schematic Concept of an Engineering Process



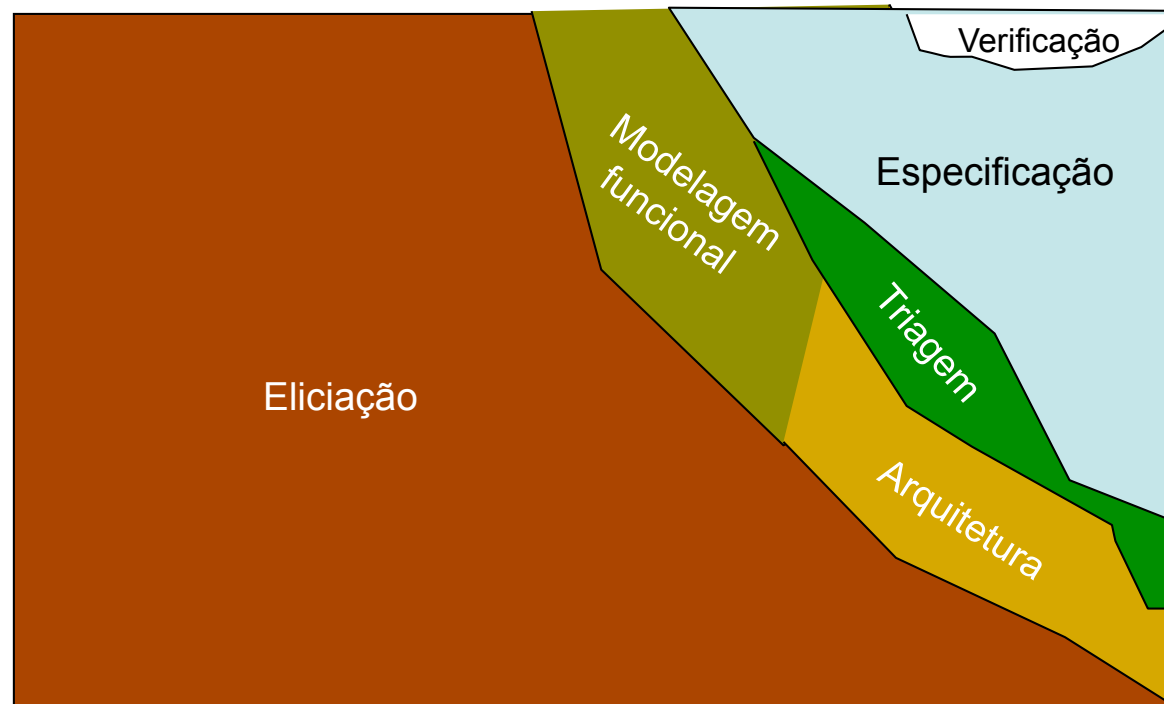
Novamente, o software



Hickey, A. M; Davis, A.M.; Requirements Elicitation and Technique Seletion: A Model for Two Knowledge-Intensive Software Engineering Process, Proc. of the 30th. Hawaian Int. Conf. on Systems Science, 2003



Fases do ciclo de requisitos de sistemas





Algumas linguagens conhecidas

PSL – Program Statment Language
U. Michigam, ISDOS Inc.

SADT – Structured Analysis and Design Technique
MIT

EDDA - (formalização do SADT e comercialização)





Algumas linguagens conhecidas

SAAM – Systematic Activity Modelling Method

Boeing Computer Services Co.

HOS – High Order Software

High Order Software Inc.





Resultados

	PSL	SADT	EDDA	SAMM	HOS	RSL
ABSTRACTION OF THE REAL WORLD						
User Familiarity of the Specification Language	×	√×	√×	×	×	×
Language Style						
• Textual language	√	×	√	×	√	√
• Graphical language	√×	√	√	√	√	√
• Hybrid languages	√	×	√	√×	√	√
Complexity						
• Separation of logical and physical characteristics	√	√×	√×	√	√	√
• Multi-level abstraction	√	√	√	√	√	√×
Modifiability	√	√	√	√	√	√
MANIPULATION OF REPRESENTATIONS						
Tools for Manipulation						
• Formalism	√	√×	√	√	√	√
• Rigour	×	×	√	√	√	√
Transformation						
• Support of different development situations	√	√×	√	√	√	√
• Transparency of formalism	×	√×	×	√	√×	√
Independence of Design and Implementation	√	√×	√×	√	√	√
CONSTRUCTION OF REAL SYSTEM						
Traceability between Specification and Target Systems	√	√	√	√	√	√



LEGION:	√	Supported
	√×	Partially supported
	×	Not supported





Atributos

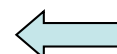
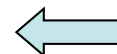
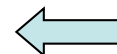
- **No. Attribute Values**

- 1 paradigm state machine, algebra, process algebra, trace
- 2 formality informal, semi-formal, formal
- 3 graphical representation yes, no
- 4 object-oriented yes, no
- 5 concurrency yes, no
- 6 executability yes, no
- 7 usage of variables yes, no
- 8 non-determinism yes, no
- 9 logic yes, no
- 10 provability yes, no
- 11 model checking yes, no
- 12 event inhibition yes, no



Comparação entre métodos

method name	paradigm	formality	graphical representation	object-oriented
Action Systems	state transition	formal	no	no
B	state transition	formal	no	no
CASL	algebra	formal	no	yes
Cleanroom & JSD	traces & process algebra	formal	yes	no
COQ	state transition	formal	no	no
Estelle	state transition	formal	no	no
LOTOS	process algebra	formal	no	yes
OMT & B	state transition	formal	yes	yes
Petri Nets	state transition	formal	yes	no
Petri Nets with Objects	state transition	formal	yes	yes
SART	state transition	informal & semi-formal	yes	no
SAZ	state transition	semi-formal & formal	yes	no
SCCS	process algebra	formal	no	no
SDL	state transition	formal	yes	yes
UML	state transition	informal & semi-formal	yes	yes
VHDL	state transition	formal	no	no
Z	state transition	formal	no	no





Atributos dos métodos

Frappier, M, Habrias, H.: A Comparison of the Specification Methods, Univ. de Sherbrook, Québec, Ca.

method name	concurrency	executability	usage of variables	non-determinism
Action Systems	no	yes	yes	yes
B	no	yes	yes	yes
CASL	no	yes	yes	no
Cleanroom & JSD	no	yes	yes	yes
COQ	no	yes	yes	yes
Estelle	yes	yes	yes	no
LOTOS	yes	yes	yes	yes
OMT & B	no	yes	yes	yes
Petri Nets	yes	yes	no	yes
Petri Nets with Objects	yes	yes	yes	yes
SART	yes	no	no	yes
SAZ	no	yes	yes	yes
SCCS	yes	yes	yes	yes
SDL	yes	yes	no	yes
UML	yes	no	no	no
VHDL	yes	yes	yes	no
Z	no	yes	yes	yes

Table 3. List of specification method attributes - part 2



Atributos dos métodos

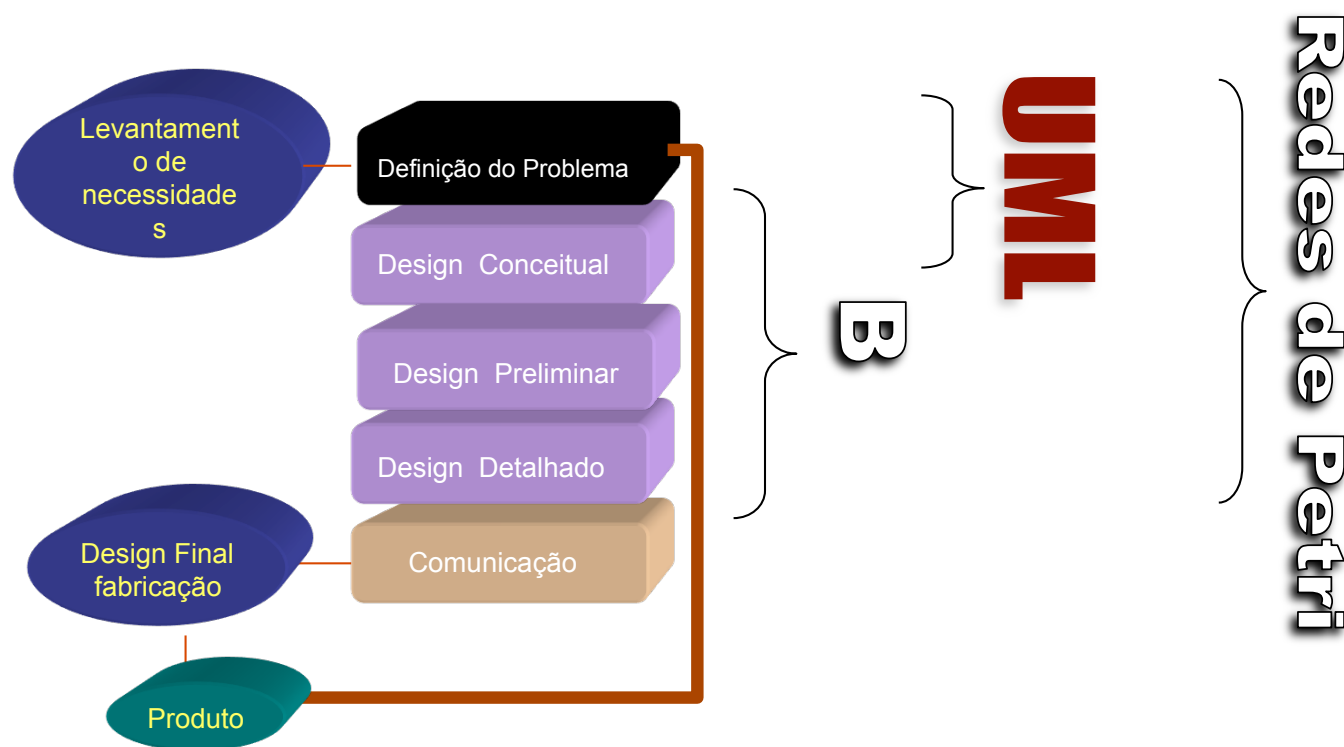
Frappier, M, Habrias, H.: A Comparison of the Specification Methods, Univ. de Sherbrook, Québec, Ca.

method name	logic	provability	model checking	event inhibition
Action Systems	yes	yes	yes	yes
B	yes	yes	yes	no
CASL	yes	yes	yes	no
Cleanroom & JSD	yes	yes	yes	no
COQ	yes	yes	yes	no
Estelle	no	no	yes	yes
LOTOS	yes	yes	yes	yes
OMT & B	yes	yes	yes	no
Petri Nets	no	yes	yes	no
Petri Nets with Objects	no	yes	yes	no
SART	no	no	no	no
SAZ	yes	yes	yes	no
SCCS	yes	yes	yes	yes
SDL	yes	yes	yes	yes
UML	no	no	no	no
VHDL	no	no	yes	no
Z	yes	yes	yes	no

Table 4. List of specification method attributes - part 3



Em busca da linguagem ideal





B e seus Antecedentes

- 1949 Alan M. Turing, Checking a large routine, Cambridge University
- 1967 Robert Floyd, Assigning meanings to programs, AMS
- 1969 C.A.R. Hoare, An axiomatic basis for computer programming, CACM
- 1972 D.L. Parnas, A Technique for Software Module Specification with Examples, CACM
- 1975 Edsger Dijkstra, Guarded commands, nondeterminacy and formal derivation of programs, CACM
- 1981 David Gries, The Science of Programming, Springer, 1981
- 1986 Roland Backhouse, Program Construction and Verification, Prentice-Hall, 1986
- 1986 Cliff B. Jones, Systematic Software Development using VDM, Prentice-Hall
- 1988 C.A.R. Hoare, Jifeng He, Natural transformations and data refinement, PRG, Oxford
- 1990 C. Morgan, Programming from Specifications, Prentice-Hall
- 1996 J.R. Abrial, The B-Book, Assigning programs to meanings, Cambridge University Press
- 1996 25-26-27 novembre, First B conference in Nantes (France)



Principais atributos

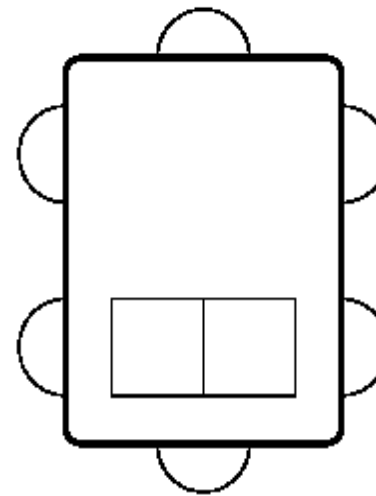
A linguagem B contém nos seus atributos:

- a formalização sound das especificações mantendo mecanismos de prova para ações e refinamentos (horizontal e vertical)
- a linguagem B incorpora o conceito de estruturação,
- separation of concerns, encapsulamento e objetos



A máquina virtual

**MACHINE ...
VARIABLES ...
INVARIANT ...
INITIALISATION ...
OPERATIONS ...
END**





...mais especificamente

```
MACHINE  $M(X, u)$ 
CONSTRAINTS  $C$     /* spécification des paramètres */
SETS  $S$ ;           /* ensembles donnés */
                $T = \{a, b\}$  /* ensembles énumérés */
CONSTANTS  $c$        /* liste de constantes (concrètes) */
PROPERTIES  $R$       /* spécification des constantes */
VARIABLES  $x$        /* liste de variables (abstraites) */
INVARIANT  $I$        /* spécification des variables */
INITIALISATION  $U$  /* substitution d'initialisation */
OPERATIONS      /* liste des opérations */
                $r \leftarrow nom\_op(p) = \text{PRE } P \text{ THEN } K \text{ END}; \dots$ 
END
```



Estratégia de modelagem

A base para a modelagem de um sistema em B é a máquina abstrata. Em outras palavras, a modelagem de um sistema é uma associação lógica de máquinas abstratas onde:

- vale o princípio da composicionalidade, isto é, uma associação de máquinas abstratas é também uma máquina abstrata;
- Cada máquina encapsula sua capacidade na forma de operações que pode realizar e se assemelha a um objeto (com herança simples e agregação);
- Existe uma arquitetura hierárquica entre as máquinas abstratas



Base para a modelagem

A base para a modelagem é a teoria de conjuntos onde se destacam os conjuntos e as expressões.

$S_1 \times S_2$

Produto cartesiano

$\mathbb{P}(S)$

Conjunto das partes

$\{x \mid P\}$

Regra de composição interna

BIG

Um conjunto infinito



■ ■ ■

x

Variável

$[x := E_1]E_2$

Substituição em uma expressão

(E_1, E_2)

Um par de expressões

$\text{choice}(S)$

Função de escolha

S

Um conjunto



Base do formalismo lógico

Lógica de predicados

$$P \wedge Q, P \Rightarrow Q, \neg P$$

Predicados base

$$\forall x \cdot P$$

Quantificador universal

$$[x := E] P$$

Substituição em um predicado

Outros predicados envolvendo conjuntos

$$x \in S$$

Relação de pertinência

$$E_1 = E_2$$

igualdade

As demais relações se formam como uma combinação das anteriores

$$P \vee Q, \exists x \cdot P, x \notin S, \text{ etc.}$$



Exemplo: um elevador

- uma porta em cada andar
- os comandos vindos do interior ou da parte externa são iguais
 - não existem falhas
- o número máximo de andares é $\text{max_andar} > 0$

As operações sobre o elevador são:

- abrir e fechar a porta
- chamar o elevador
- deslocar o elevador





Propriedades do elevador

- o elevador se move no limite dos andares 0 (térreo) e max_andar ;
- a porta de um dado andar só se abre se o elevador estiver neste mesmo andar;
- cada chamada deve ser atendida dentro de um certo intervalo de tempo t_{max} ;
- se o elevador chega a um andar a chamada vinda deste andar é considerada atendida.



Máquina abstrata

MACHINE: Elevador;

SETS : ESTADO = {parado, movimentando};

CONSTANTES : max_andar, ANDARES;

PROPRIEDADES: $\text{max_andar} \in \text{NAT}^* \wedge \text{ANDARES} = 0..\text{max_andar}$;

VARIÁVEIS : chamada, pos, porta_aberta $\in$ ANDARES
estado $\in$ ESTADO;

INVARIANTES: $(\text{estado}=\text{parado} \Rightarrow \text{chamada} = \text{porta_aberta} \vee$
 $\text{estado}=\text{movimentando} \Rightarrow \text{chamada} \neq \text{porta_aberta})$;

OPERADORES: $(\text{porta_aberta}=\text{max_andar}) \Rightarrow (\text{destino} = \text{max_andar} - 1)$

$(\text{porta_aberta}=0) \Rightarrow (\text{destino} = 1)$;

$[(\text{porta_aberta} > 0) \wedge (\text{porta_aberta} < \text{max_andar})] \Rightarrow [(\text{destino}=\text{porta_aberta} + 1) \vee$
 $(\text{destino}=\text{porta_aberta} - 1)]$



“ATELIER DE
GENIE LOGICIEL...”

[Home](#) - [News](#) - [Products](#) - [Versions](#) - [Download](#) - [Manuals](#) - [Maintenance](#) - [Distribution Policy](#) - [Roadmap & Contribution](#) - [Support](#) - [Training](#) - [Documents](#) - [Press](#) - [References](#) - [R&D](#) - [Contacts](#) - [Jobs](#) - [Links](#) - [Your Account](#)  

Search

Atelier B, the industrial tool to efficiently deploy the B Method

▶ ATELIER B PRESENTATION

Developed by **ClearSy**, **Atelier B** is an industrial tool that allows for the operational use of the B Method to develop defect-free proven software (formal software).

It is used to develop safety automatisms for the various subways installed throughout the world by Alstom and Siemens, and also for

▶ WHY USE ATELIER B 4.0 ?

▶ Free Download

▶ New Distribution Policy

▶ New Maintenance Contract

+ More





Atelier B - Download

Knowledge engineering - ... x IEEE Xplore - Knowledge a... x Atelier B - Download x SciELO - Scientific Electron... x +

http://www.atelierb.eu/php/telecharger-atelier-b-en.php

Most Visited Getting Started Latest Headlines Apple Yahoo! Google Maps YouTube Wikipedia Bookmarks

GAME & APPS B atelier B Web Search Login

ATELIER B

"ATELIER DE GENIE LOGICIEL..."

Home - News - Products - Versions - Download - Manuals - Maintenance - Distribution Policy - Roadmap & Contribution - Support - Training - Documents - Press - References - R&D - Contacts - Jobs - Links - Your Account  

Search

Download Atelier B

Download Atelier B Files...

 **Atelier B 4.0**

- ▶ Atelier B 4.0 - Windows
- ▶ Atelier B 4.0 - Linux
- ▶ Atelier B 4.0 - Mac OS
- ▶ Atelier B 4.0 - Solaris

 **Oldest Versions of Atelier B**

These versions of Atelier B, formerly on the market, are no longer available except in certain conditions. Contact us if necessary contact@atelierb.eu

- ▶ Atelier B 3.7.2

Trash

MICRONICA





B Site pages

Knowledge engineering - ... x IEEE Xplore - Knowledge a... x B Site pages x SciELO - Scientific Electron... x +

http://vasco.imag.fr/B/Bsite-pages.html

Most Visited Getting Started Latest Headlines Apple Yahoo! Google Maps YouTube Wikipedia Bookmarks

GAME & APPS B Grenoble Web Search

Site B Grenoble
Grenoble Site

Actualités de B **B News**

B News

Documents on B

Conferences / Meetings

B Tools

B Industrial Gateway

B Projects

B Academic World

French B Working Group

Mailing List

Links

Contact Didier.Bert@imag.fr for further information.

ABZ 2010

February 23-25, 2010, Oxford, Québec, Canada

Important dates:

September 21, 2009 : Submission of full papers

October 11, 2009 : Submission of extended abstracts for short presentations

November 3, 2009 : Notification

November 17, 2009 : Final Version

February 23-25, 2010 : Conference

February 22, 2010 : Tutorials and Workshops

From Research to Teaching Formal Methods - The B Method

8 June 2009, Nantes (France)

Important dates:

March 20, 2009: Submission of full papers

April 24, 2009: Notification of acceptance/rejection of submitted papers.

Offre d'emplois à la RATP

[22 August 2008]

Téléchargez / Download : [Descriptif \(.doc\)](#)

Offre d'emplois à Siemens

[8 March 2008]

Téléchargez / Download : [Data d'information L'Engineering \(.pdf\)](#)

Trash

IMAG

MECATRONICA



B Site pages

Knowledge engineering - ... x IEEE Xplore - Knowledge a... x B Site pages x SciELO - Scientific Electron... x

http://vasco.imag.fr/B/Bsite-pages.html

Most Visited Getting Started Latest Headlines Apple Yahoo! Google Maps YouTube Wikipedia Bookmarks

GAME & APPS B Grenoble Web Search Login

Site B Grenoble

Outils sur B **B Tools**

Comments on tools, experiments, comparisons,... are welcome on the [B forum](#)

Outils industriels / Industrial Tools

- [Atelier-B](#)
- [B4free tools](#)
B4free is a set of tools for the development of B models and for creation of user tools. It can be used through the Click'n'Prove interface.
- **EmacsPri** [French version](#) [English version](#)
Interface Emacs du prouveur interactif Version 1.7.3
Xemacs Interactive Prover Interface Version 1.7.3
(Freeware)
- [B-toolkit](#)

Outils universitaires / Academic Tools

- [GeneSyst and BoB](#)
"GénéSyst" is a tool that takes a B event system and a partition of the B state as input and, as output, generates a symbolic finite-state automata where "states" are the substates defined by the user in input, and transitions are labeled by the events. Transitions also contain information about raising and reaching conditions (see

Contact Didier.Bert@imag.fr for further information.



B Site pages

Knowledge engineering - ... x IEEE Xplore - Knowledge a... x B B Site pages x SciELO - Scientific Electron... x +

http://vasco.imag.fr/B/Bsite-pages.html

Most Visited Getting Started Latest Headlines Apple Yahoo! Google Maps YouTube Wikipedia Bookmarks

GAME & APPS B grenoble Web Search

Site B Grenoble
Grenoble Site

[B News](#)
[Documents on B](#)
[Conferences / Meetings](#)
[B Tools](#)
[B Industrial Gateway](#)
[B Projects](#)
[B Academic World](#)
[French B Working Group](#)
[Mailing List](#)
[Links](#)

Contact Didier.Bert@imag.fr for further information.

Portail des industriels

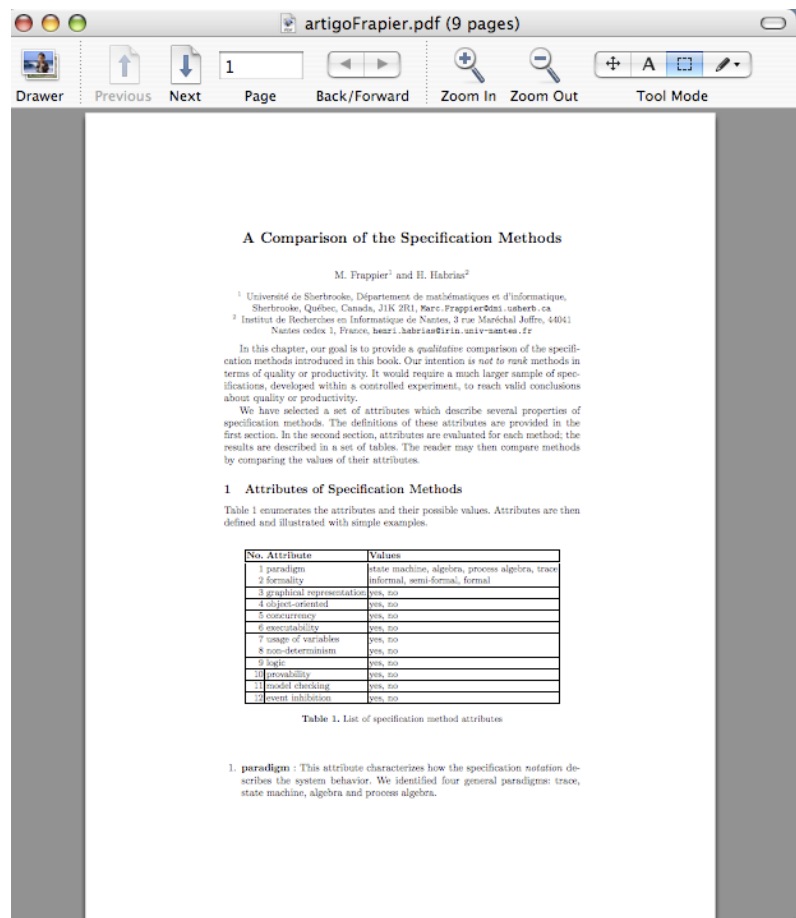
Industrial Gateway

[[Industrial Users](#) | [Job Offers](#) | [Training Period Offers](#)]

Utilisateurs industriels de B / B Industrial Users

GEMALTO Contact Boutheina Chetali	CLEARSY Contact Thierry Lecomte 1330 rue G. de la Lauzière F-13856 Aix-en-Provence Cedex
SIEMENS Transportation Systems Contact Daniel Dollé 48-56 rue BARBES BP 531 F-92542 Montrouge Cedex	KEESDA Contact Jean Mermet Parc Equation 2, avenue de Vignate F-38610 Gières
ALSTOM Transport Contact Luiz Fernando Mejia 33, rue des Bateliers F-93400 Saint-Ouen	SYSTEREL Contact Jean-Frédéric Roal Portes de L'Arbois bat A, 1090, rue Ren Descartes Parc d'activités La Duranne 13857 AIX-en-PROVENCE Cedex 3
LEIRIOS technologies Contact R&D TEMIS Innovation 18 Rue Alain Savary 25000 BESANCON	







Exercício

Exercício desta semana consiste, em, usando o artigo recomendado (e eventualmente outros sugeridos por vocês) discutir o uso de representações (formais, semi-formais, formais) no tema escolhido como trabalho final. O resultado do exercício, dependendo do caso e do tema, pode até ser uma justificativa para não usar linguagens (formais), o que importa é que isso seja uma decisão consciente do projeto.



Fim