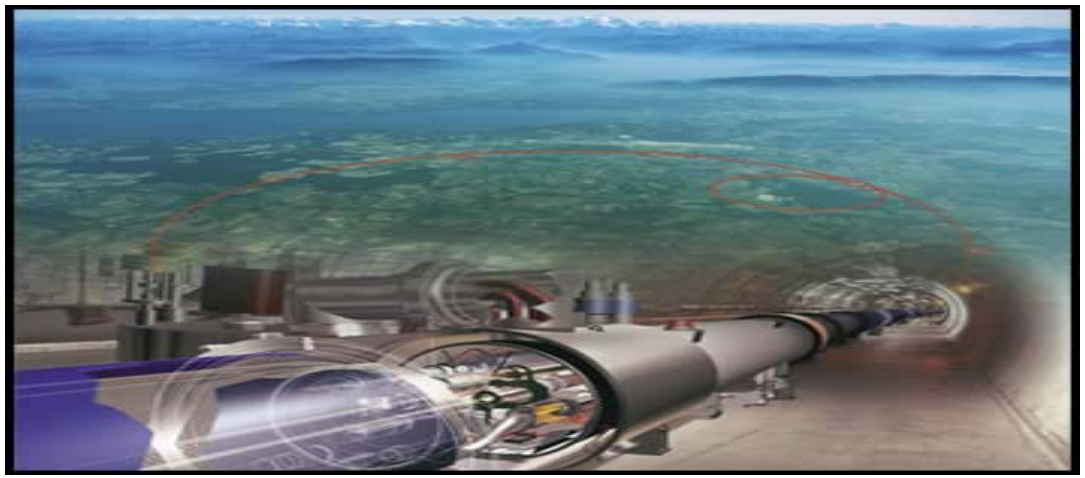
Curso de Especialização e Mestrado em Informática

Especificação Reversa e Reengenharia de Software: estudo de caso



Seminário

Braga, 13 de Janeiro de 2006

David Sora – CERN

Sumário

- CERN
- Experiência COMPASS e o DCS
- Reengenharia do DCS
  - Motivação
  - Reverse and Forward Engineering
  - Métodos Formais
    - Sub-sistema STRAWS
    - Especificação Reversa
    - Processo de especificação
    - Detecção de inconsistências
    - Estrutura orientada ao objecto
    - Animação com o VDM++ Interpreter
- Conclusões e trabalho futuro

CERN

O que é o CERN?

- **European Organization for Nuclear Research:** um dos maiores laboratórios científicos do mundo;
- **Onde?** Junto da cidade de Genebra, sendo atravessado pela fronteira franco-suiça;
- **Ciência pura:** Física de partículas

Procuram-se respostas para várias perguntas universais e não só…

- Do que é feita a matéria?
- O que a mantém coesa?
- Para onde foi a anti-matéria?
- …
- Quem nasceu primeiro, a galinha ou o ovo?!!!!!!!!!!

- **Instrumentos:** Aceleradores e Detectores;

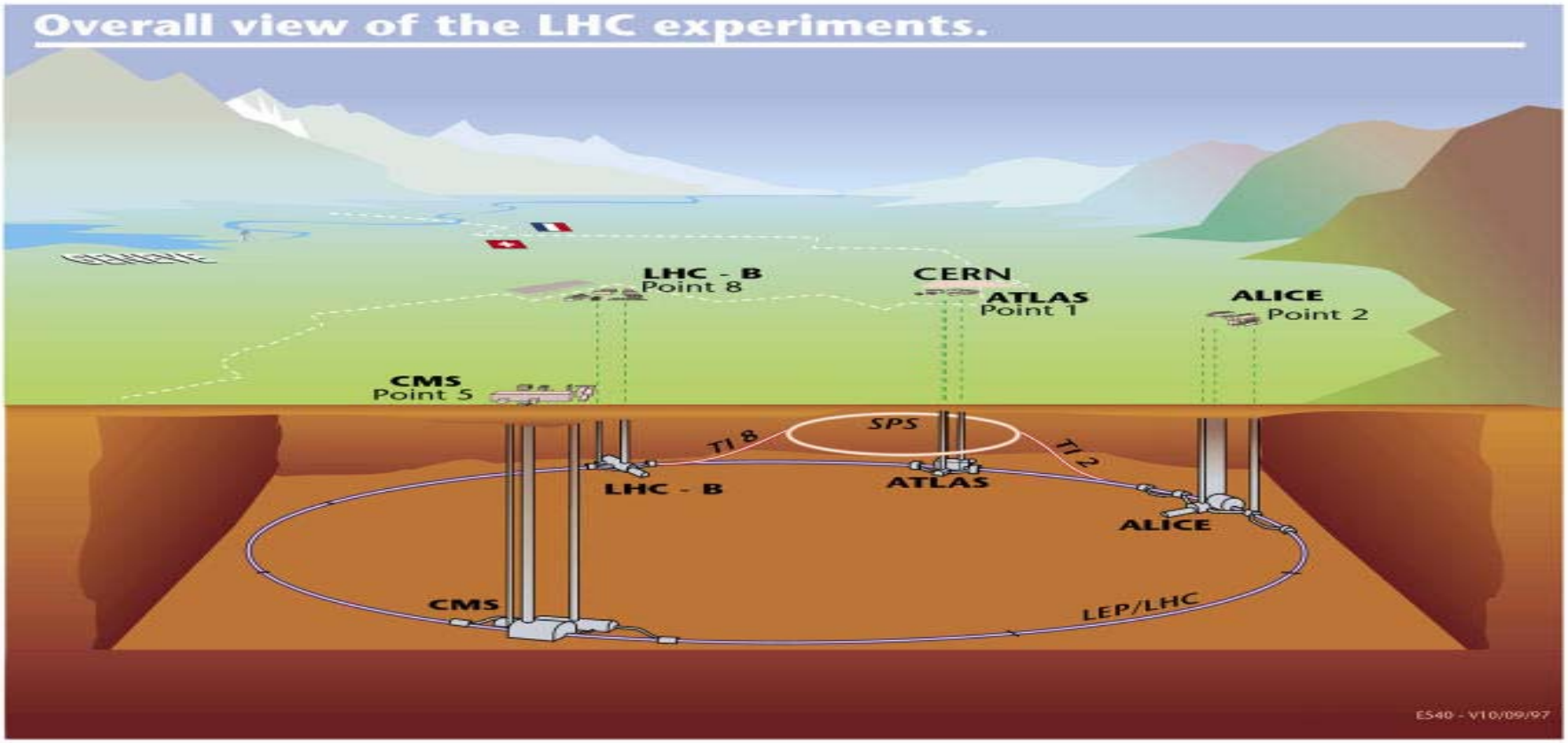
CERN

Localização

Fotografia: vista aérea do espaço ocupado pelo túnel do LHC

CERN

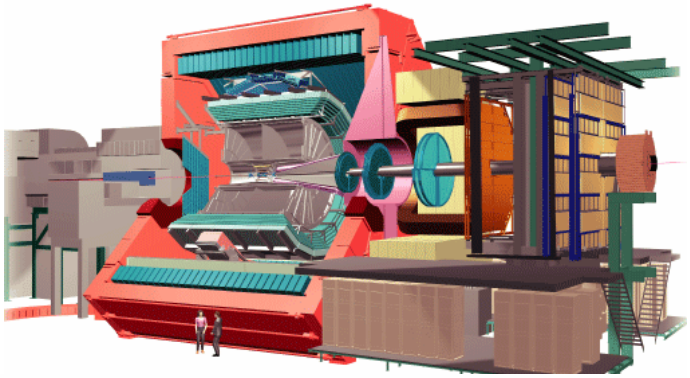
Localização



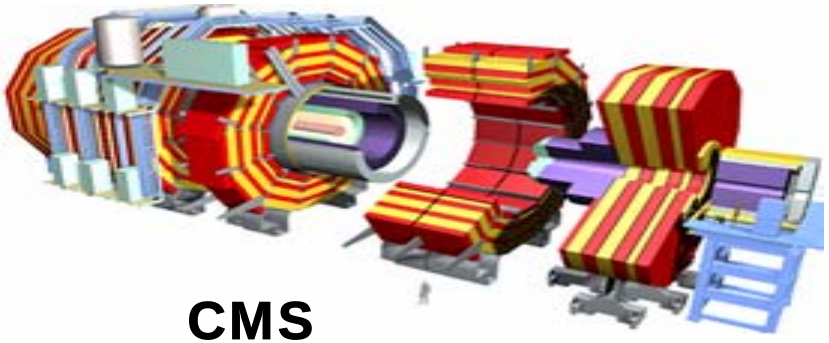
Vista geral das experiências LHC

CERN

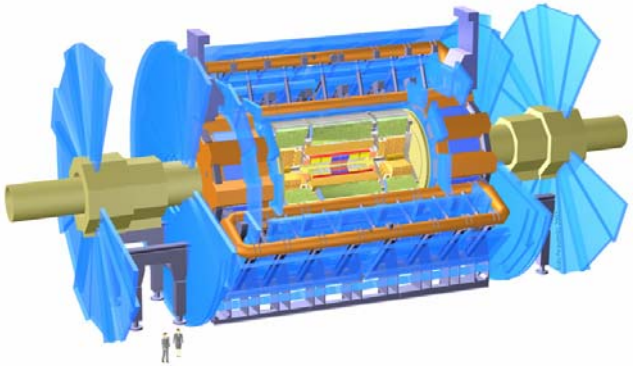
Detectores



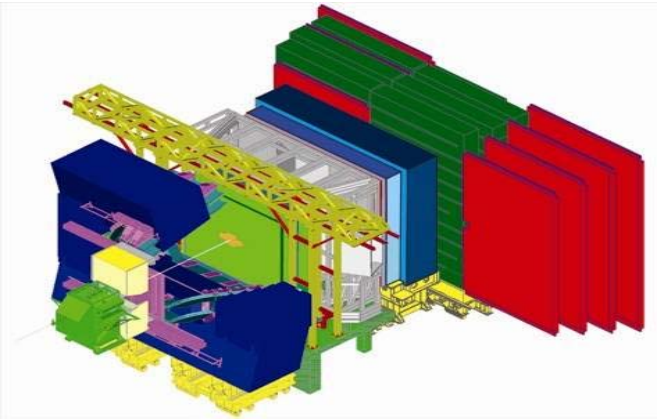
ALICE



CMS



ATLAS



LHC-B

CERN

Aceleradores

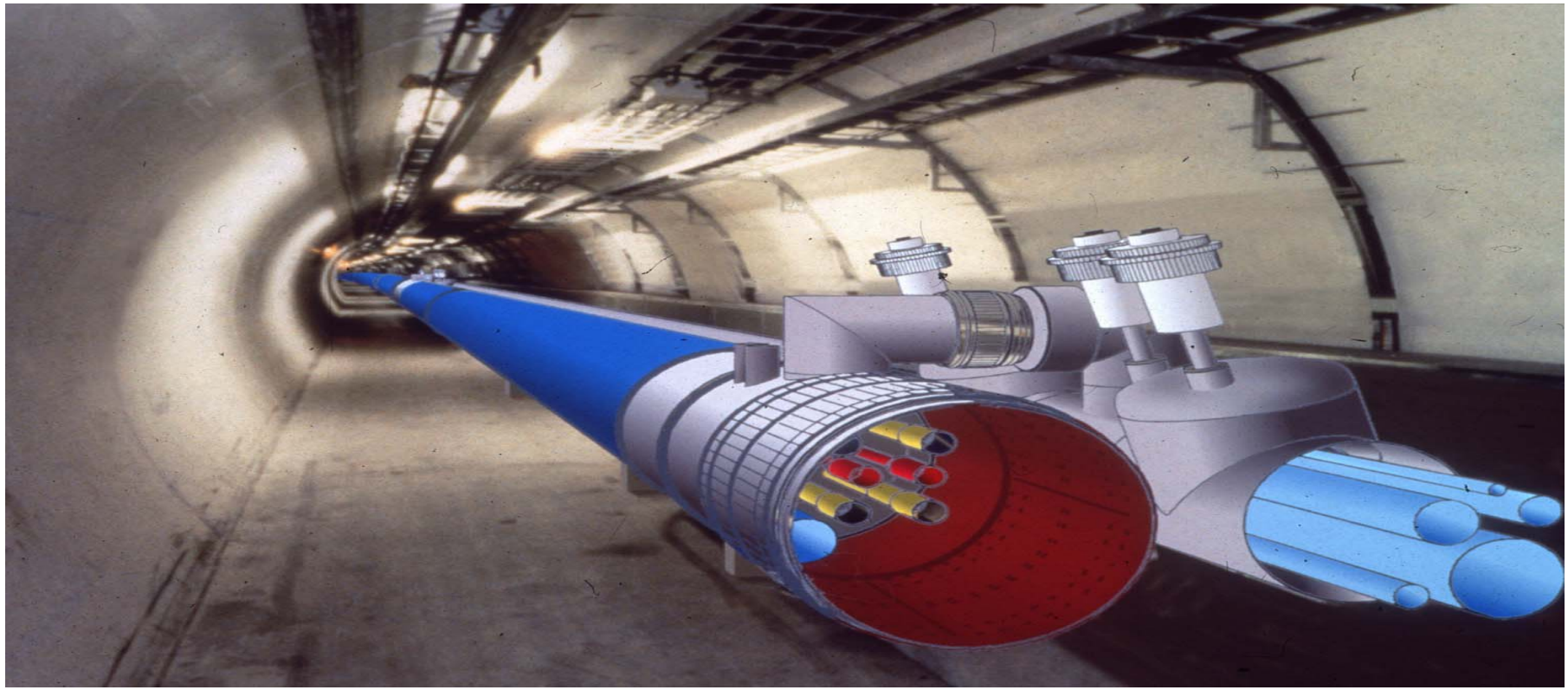


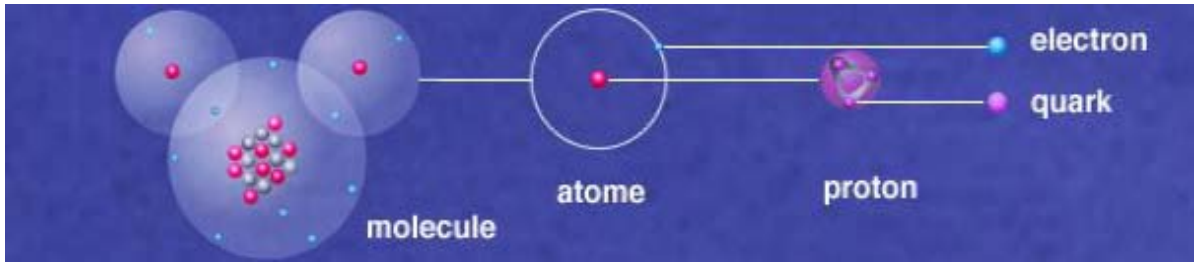
Imagem virtual mostra o LHC (Large Hadron Collider accelerator) tal como deverá ser num túnel real do CERN, em 2007…

CERN

Porquê o estudo das partículas?

- Tudo, no Universo é feito a partir de um pequeno número básico de blocos chamados **Partículas Elementares**, governados por algumas forças elementares.

a) Partículas estáveis
b) Partículas *não-estáveis*



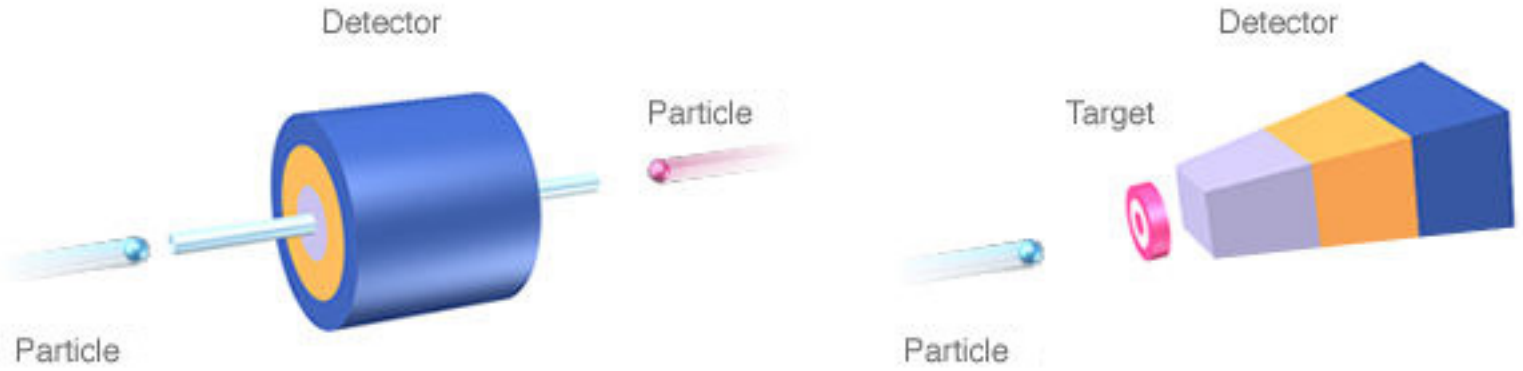
- **Big Bang:** a) e b) coexistiram alguns instantes após o Big Bang
- **Aceleradores do CERN:** « máquinas do tempo »… recriam o mesmo ambiente existente aquando da origem do Universo.

- **Porquê?**

  Para **compreender** a **formação das estrelas**, **da terra**, **árvores**, tudo a nossa volta e finalmente **nós próprios!**

CERN

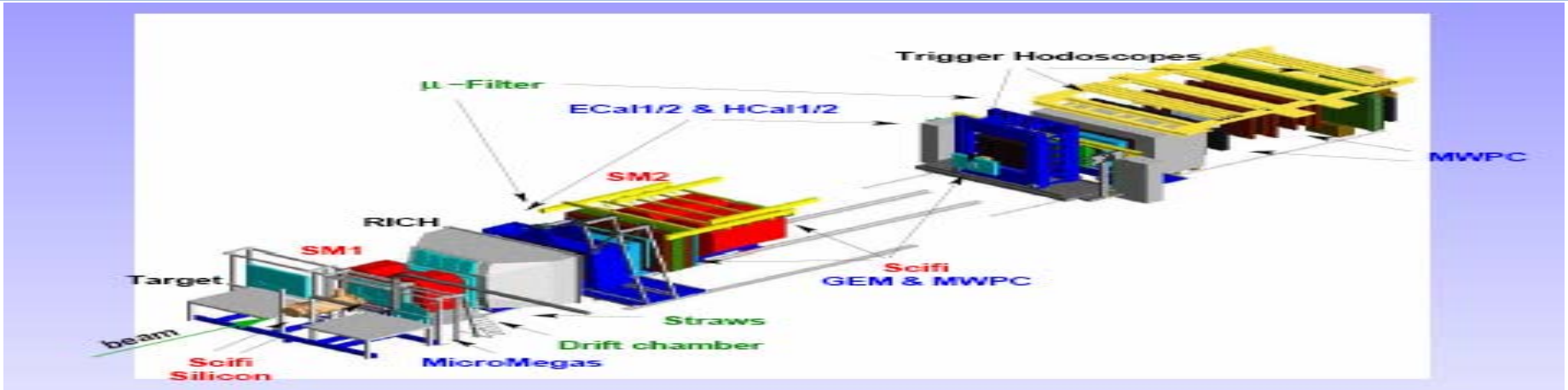
Experiências



Experiências no CERN estão divididas em duas grandes categorias:

- **Colisionadores (detectores em forma de cilindro);**
- **Alvos fixos (detectores em forma de cone).**

Experiência COMPASS e o DCS



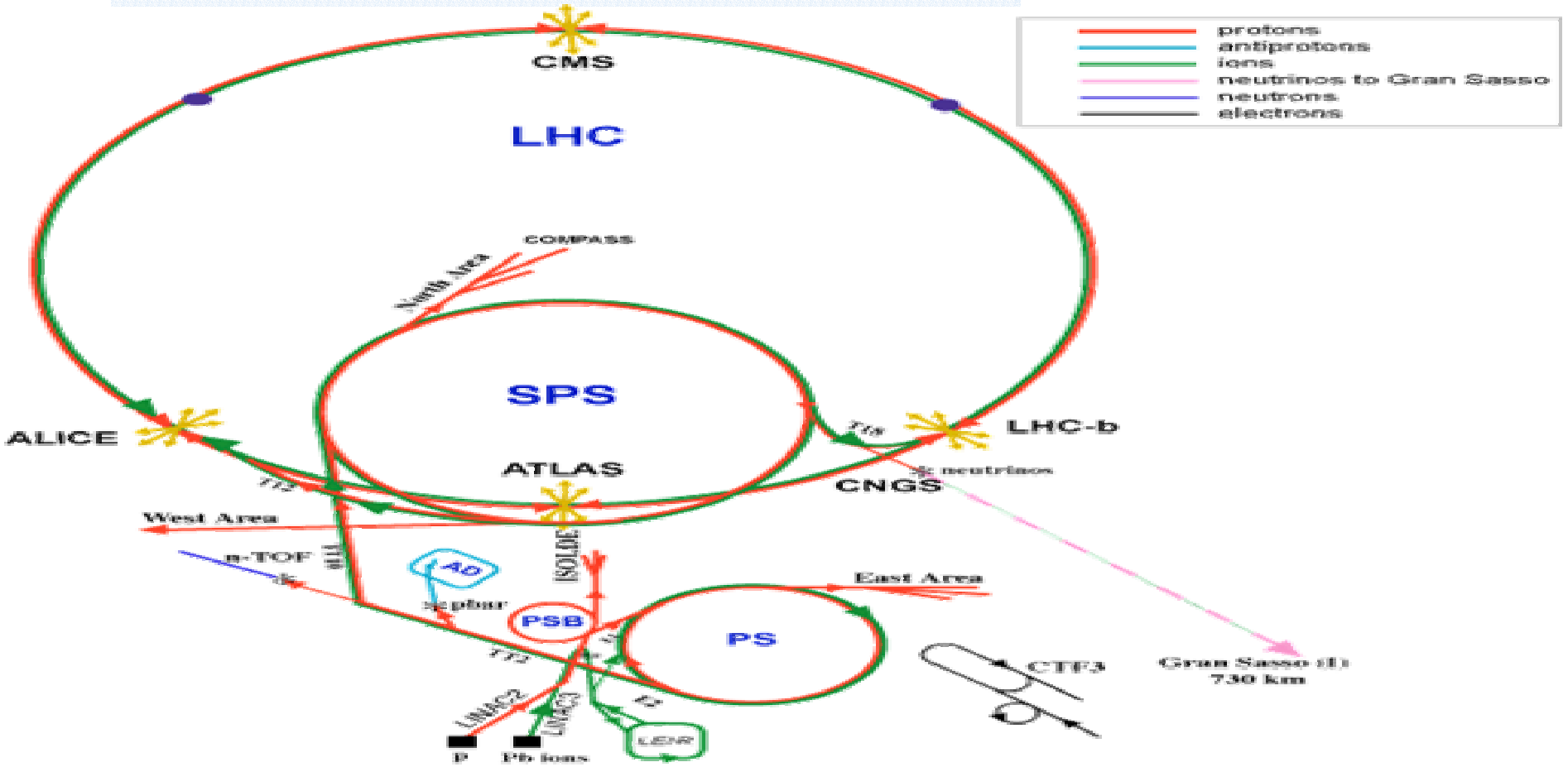
COMPASS - COmmon Muon Proton Apparatus for Structure and Spectroscopy

- **Objectivo: Estudar a estrutura do Hadrão c/feixes de alta energia (Hadrões e Muões)**
- **Espectroscopia: Estuda a interacção da luz, ou qualquer radiação electromagnética, com a matéria.**

1997 – Aprovação do projecto
2000/01 – Instalação dos detectores
2002/04 – Tomada de dados (≈ 800 TBytes)
2005 – Primeiros resultados físicos publicados
2005/06 – DCS totalmente redesenhado
2006 – Nova tomada de dados

Experiência COMPASS e o DCS

Localização



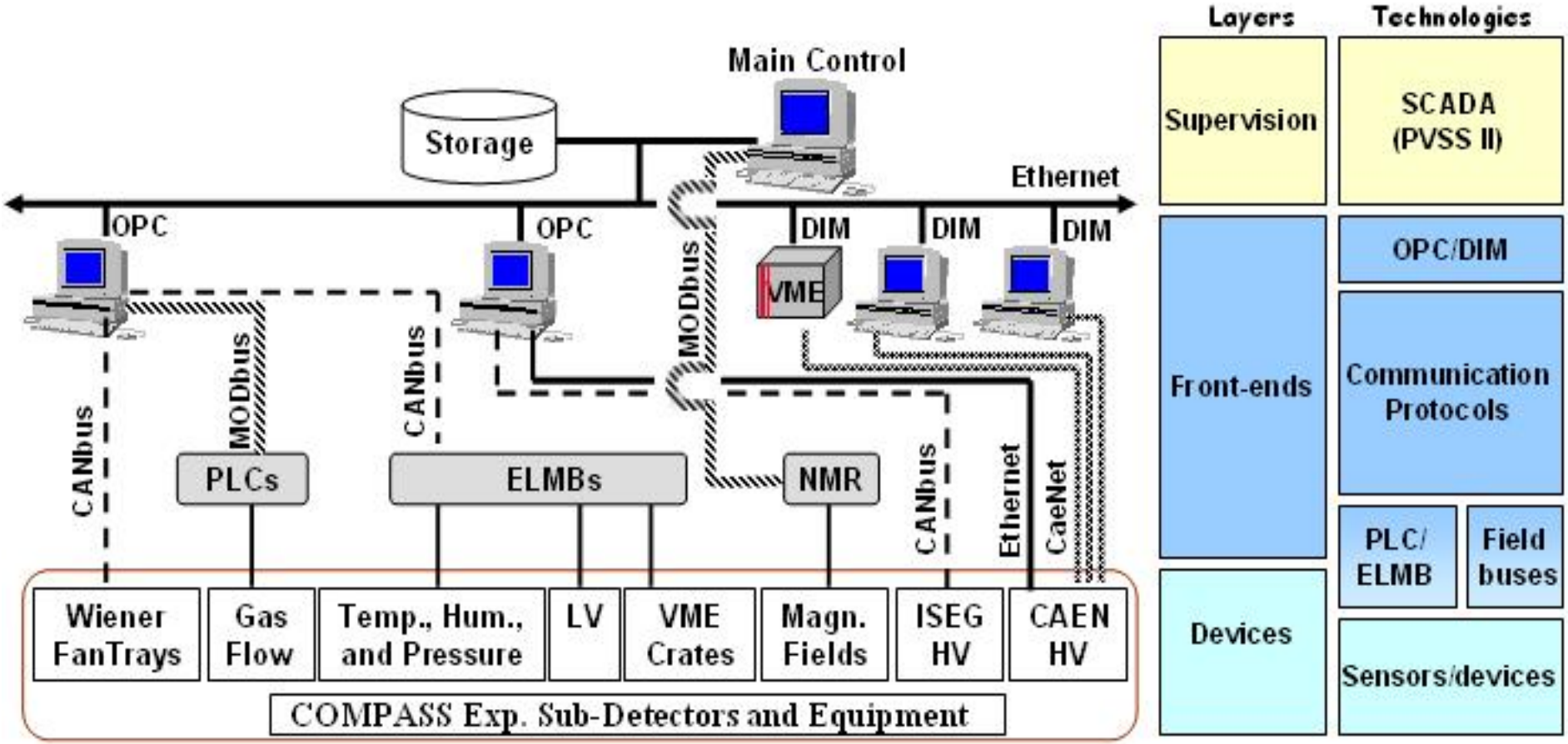
Experiência COMPASS e o DCS

DCS – Detector Control System

- Controlo dos parâmetros de funcionamento dos detectores: sistemas de alta-tensão, de baixa-tensão e *fan-trays* para os módulos de electrónica.
- Monitorização de parâmetros de ambiente: temperaturas, humidades, pressão, …; e dos fluxos de gases nas câmaras gasosas.
- Sistema de alarmes centralizado no DCS: alarmes visuais (cores), sonoros (na sala de controlo), envio de SMS e e-mails aos responsáveis pelos detectores.
- Arquivo e visualização dos valores monitizados
- Um DCS acessível remotamente
- Vários níveis de segurança e fiabilidade

Experiência COMPASS e o DCS

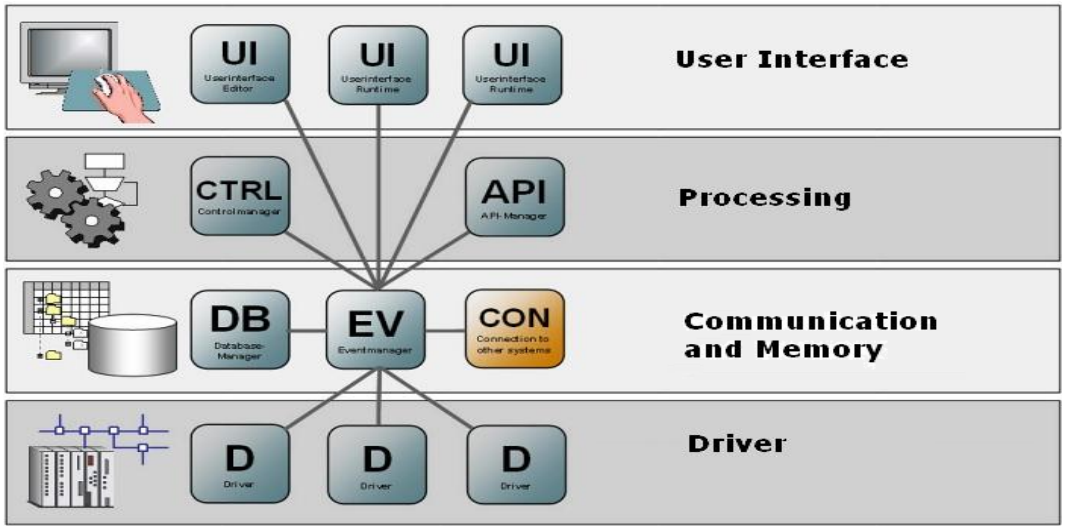
DCS – Detector Control System



Experiência COMPASS e o DCS

PVSS

- O PVSS é um produto do tipo SCADA (Supervisory Control and Data Acquisition)
  - Software comercial (austríaco)
  - Orientado ao objecto (device)
  - Sofisticado sistema de alarmes e controlo de acesso
  - Semi-aberto, escalável e flexível
  - Event-driven



- O Event Manager (EV) é responsável pela comunicação global.

Recebe dados dos Driver Managers (D) e envia-os para o DataBase Manager (DB).

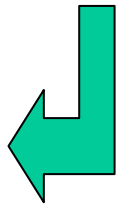
Reengenharia do DCS

Motivação

- 2005 - SPS (Super Proton Synchroton) shutdown
  - Oportunidade para redesenhar o sistema
  - Novos detectores
  - Actualização de software e hardware
  - Nova filosofia do sistema:
    - "hardware oriented" vs. "detector oriented"
  - Sistema muito complexo e crítico

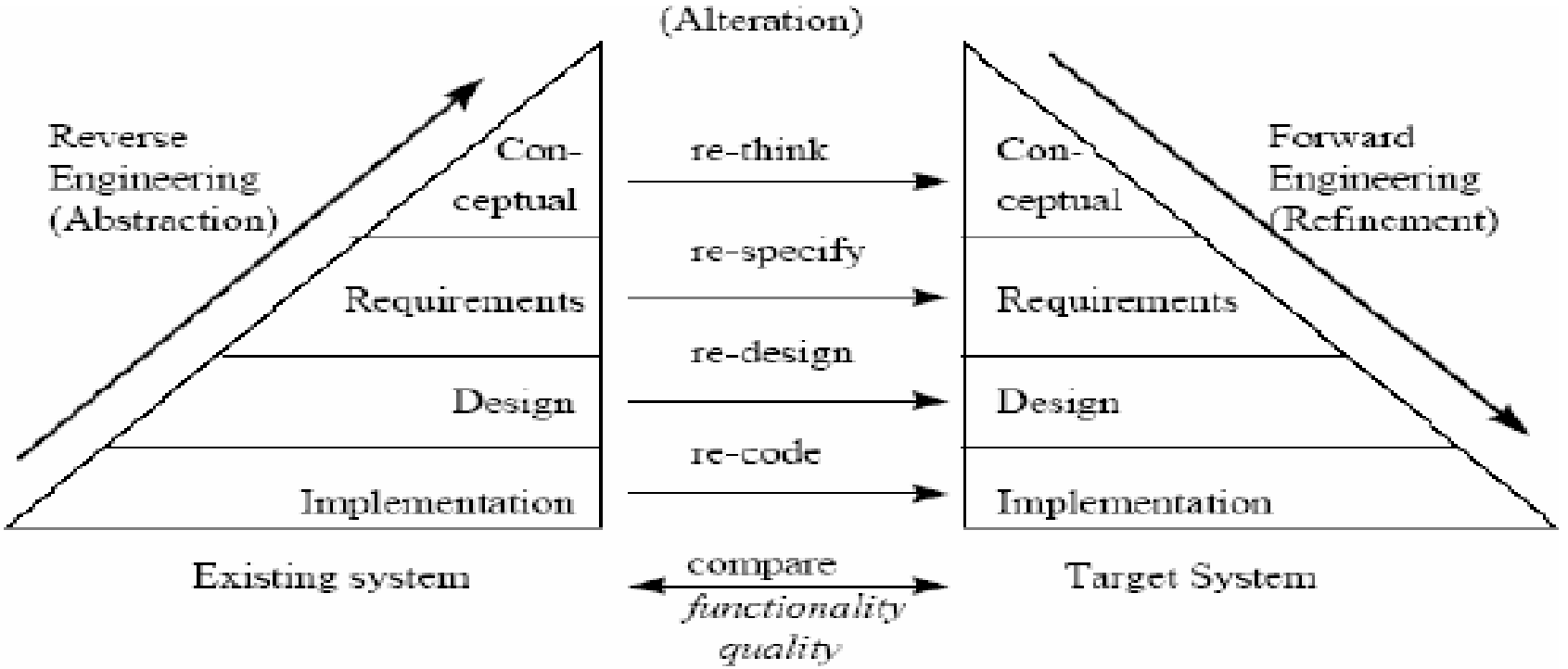
Redesenho do sistema é delicado e não trivial!!!!!

Especificação do DCS com métodos formais?



Reengenharia do DCS

Reverse and Forward Engineering



Reengenharia pode ser visto como um processo de examinação, análise e alteração de um sistema de software existente para ser posteriormente re-implementado

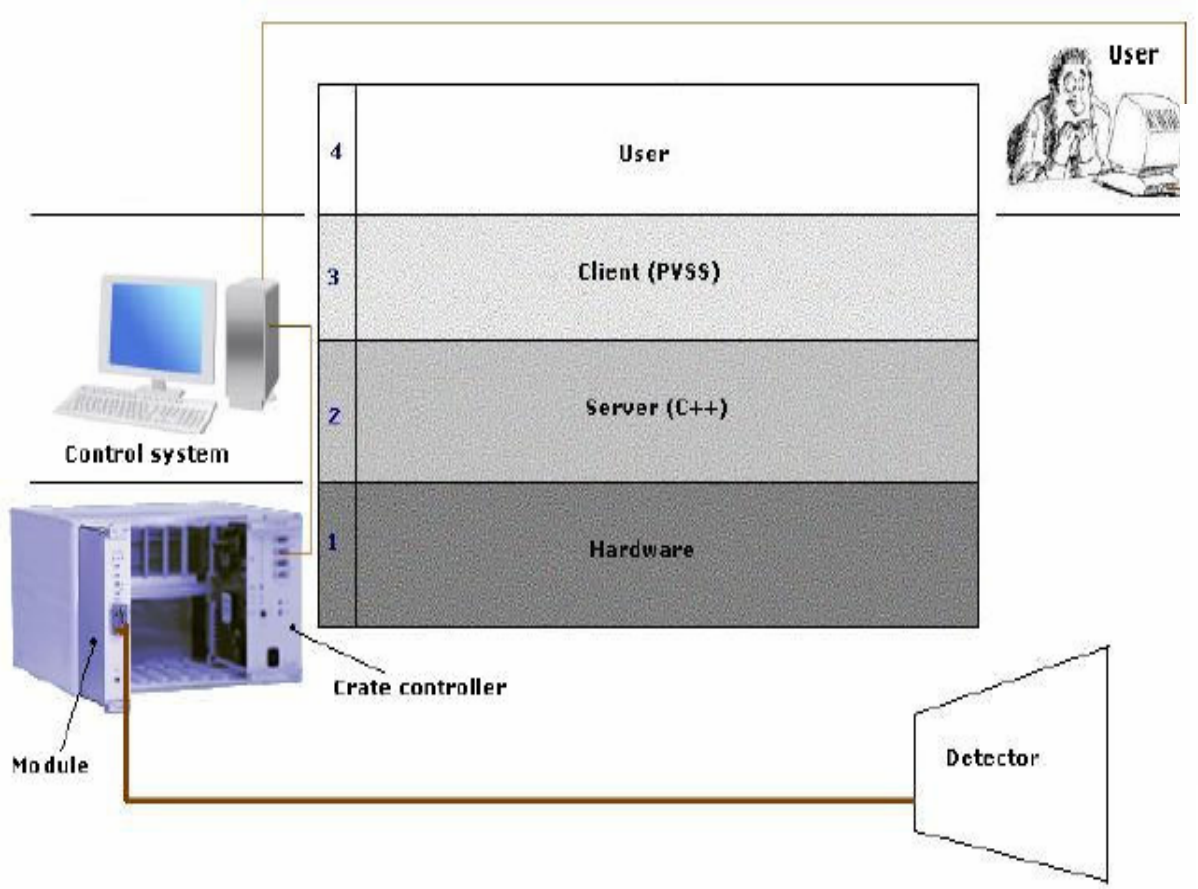
Reengenharia do DCS

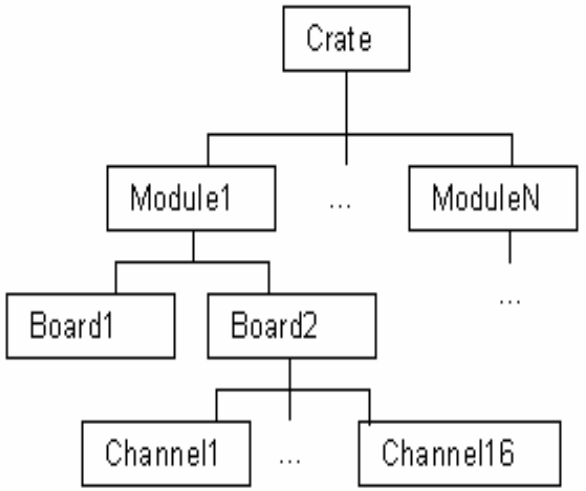
Métodos Formais

- **Construção de um modelo abstracto para o sistema**
  - **Vantagem: demonstração rigorosa do modelo**
  - **Problema: Sistema grande e muito complexo (desencoraja utilização de métodos formais)**
  - **Alternativa:**
    - **Decomposição: divisão do sistema em pequenos módulos;**
    - **Criar modelo abstracto a partir da especificação de um dos módulos;**
    - **Refinamento: a especificação do módulo escolhido para um determinado nível de abstracção inferior deve satisfazer as exigências de um nível de abstracção superior.**
  - **Alvo escolhido: sub-sistema STRAWS**
  - **Ferramentas: VDMTools (VDM-SL e VDM++)**

Reengenharia do DCS

Métodos Formais – Sub-sistema STRAWS





Structure of a Crate

Reengenharia do DCS

Métodos Formais – Especificação Reversa

- **Especificação Formal:** processo de descrever um sistema e suas propriedades.
  - Usa uma "linguagem matemática" com uma sintaxe e semântica bem definida.
  - As propriedades do sistema podem incluir:
    - Comportamentos funcionais
    - Comportamentos temporais
    - Características de performance
    - Estrutura interna

- **Especificação Reversa:** a especificação é abstraída a partir do código fonte ou da descrição do desenho do sistema.

Reengenharia do DCS

Métodos Formais – Processo de especificação

10 passos que <u>podem</u> guiar o processo de especificação:

1) Determinar o objectivo do modelo;
2) Definir os requisitos do sistema;
3) Analisar os comportamentos funcionais extraídos dos requisitos;
4) Extrair uma lista de potenciais classes/tipos de dados e operações (diccionário);
5) Criar uma representação das classes com diagramas UML;
6) Verificar as assinaturas para as operações ;
7) Completar a definição de classes/tipos de dados determinando potenciais invariantes e formalizar as mesmas;
8) Completar a definição das operações determinando pre- e pós-condições, modificando definições de tipo se necessário;
9) Validar a especificação usando testes sistemáticos;
10) Implementação do modelo usando geração automática (ou manual) de código.

Reengenharia do DCS

Métodos Formais – Processo de especificação

- **Primeira Fase:**
  - **Estudo do sistema e sua arquitectura**
  - **Processo de especificação em VDM-SL**
  - **Filosofia do sistema: hardware-oriented**
  - **Sistema existente em 2004**
- **Segunda Fase:**
  - **Análise da especificação criada na fase I**
  - **Processo de especificação em VDM++**
  - **Detectores e suas componentes vistas como objectos**
  - **Filosofia do sistema: detector-oriented**
  - **Sistema que deverá estar funcional em meados de 2006**

Reengenharia do DCS

Métodos Formais – Detecção de inconsistências

- **É FUNDAMENTAL definir invariantes logo no princípio da especificação;**
- **Uma má compreensão dos requisitos do sistema afecta de forma determinante as seguintes fases do desenvolvimento do sistema;**

- **Exemplo de um problema encontrado no sistema original, durante o processo de especificação:**
  - **O sistema permite ao utilizador de definir um valor de corrente (*C*), para um qualquer canal STRAWS de alta tensão, inferior a *cmax* (*cmax* = Limite de corrente em µAmperes);**
  - **O limite de hardware para a corrente dum canal é de 200 µAmperes;**
  - **No entanto a definição de *cmax* aceita qualquer valor do tipo *real*, ou seja, o sistema permite que o valor de *cmax* seja superior ao próprio limite de segurança definido no hardware!!**

Reengenharia do DCS

Métodos Formais – Detecção de inconsistências

- **Solução?**

Definir um tipo (*Current*) correspondente a corrente do canal, já com uma limitação associada (exemplo em VDM-SL):

```
Current = real
inv cur == cur>= 0.0 and cur <= 0.0002;
```

e definir *cmax* como sendo do tipo *Current* (exemplo em VDM-SL):

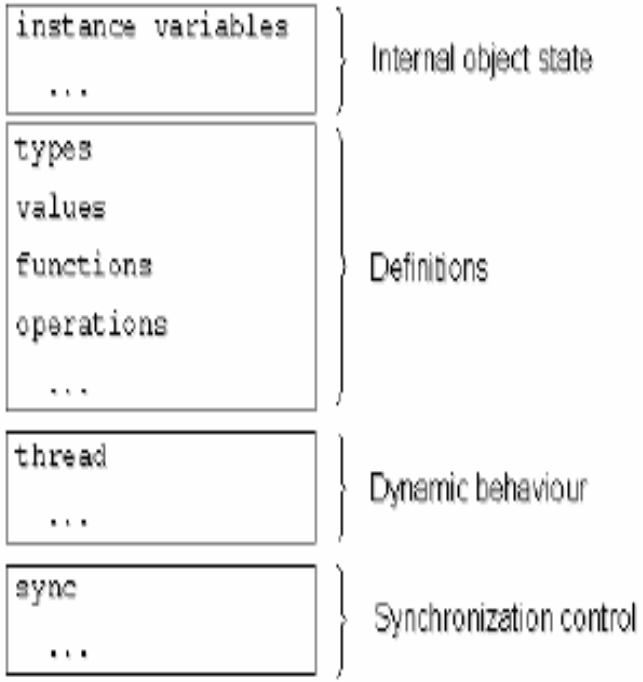
```
Channel:: idc: seq of char
V: Voltage
C: Current
S: seq of char
A: Alarm
vmax: Voltage
cmax: Current;
```

Reengenharia do DCS

Métodos Formais - Estrutura Orientada ao Objecto

Vejamos em VDM++…

```
class Channel

types

      public Voltage = real
      inv volts == volts >= 0.0 and volts <= 2500.0;

      public Current = real
      inv cur == cur >= 0.0 and cur <= 0.0002;

      public Alarm = <OK> | <Over_Current> | <Over_Voltage> | <Trip>;

instance variables

      Name: seq of char := "";
      V: Voltage := 0.0;
      VSet: Voltage := 0.0;
      C: Current := 0.0;
      S: seq of char := "";
      A: Alarm := <OK>;
      vmax: Voltage := 2500.0;
      cmax: Current := 0.0002;
      inv ChannelInv(V,vmax,C,cmax,VSet,A,S);

functions

-- ------------------------------------------
-- Invariant function for the channel
-- ------------------------------------------
```



Estrutura típica de uma classe em VDM++

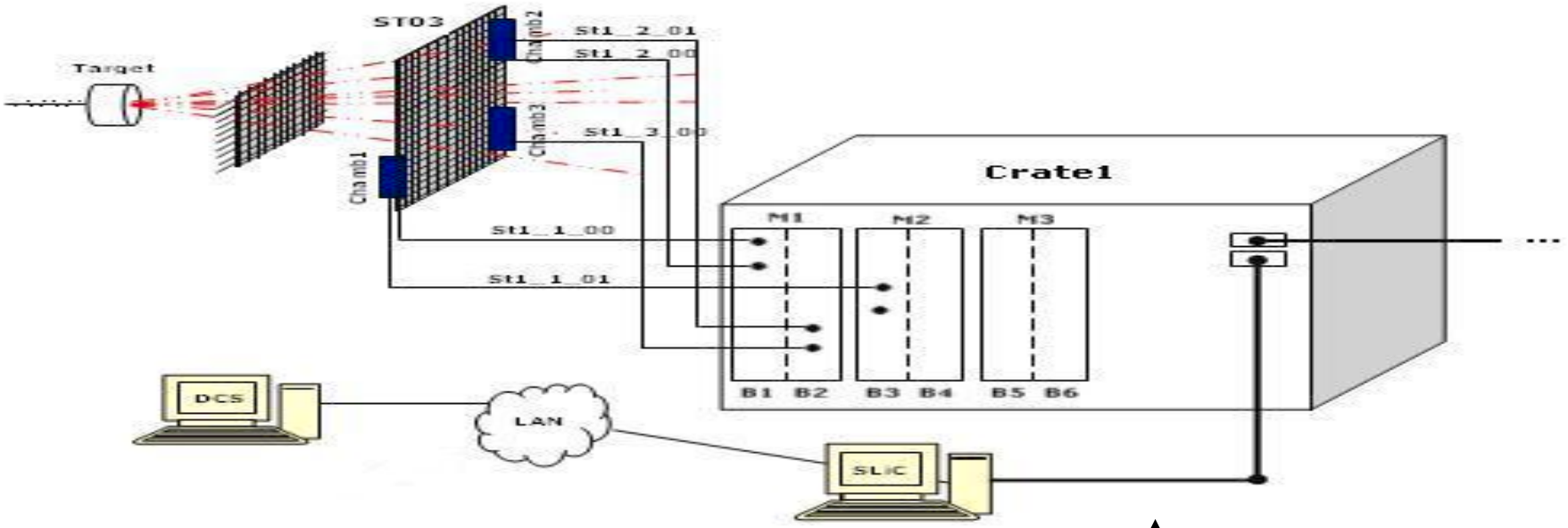
Reengenharia do DCS

Métodos Formais – Animação com o VDM++

- **Alvo do teste: pequeno conjunto de canais de alta tensão**
- **Configuração do teste:**
  1) **Definição dos objectos em ficheiros de scripts**
  2) **Setup do VDM++ Interpreter para permitir:**
     - **Dynamic type check;**
     - **Dynamic checks of invariants;**
     - **Check of pre-conditions;**
     - **Check of post-conditions**
  3) **Execução das scripts de teste para dar vida ao sistema**
  4) **Lançar comandos/verificar estados**

Reengenharia do DCS

Métodos Formais – Animação com o VDM++



	Ch00	Ch01	Ch02
Alarm	<Over_Current>	<Over_Current>	<OK>
Current	0	0	0
State	"OFF"	"OFF"	"OFF"
Voltage	0	0	0
VSet	49.9	169.9	1369.9
cmax	0.00018	0.00018	0.00018
vmax	2400	2400	2400

Ilustração do sistema simulado e seu estado inicial.

Conclusões e trabalho futuro

- **Este projecto focou a especificação reversa de um fragmento de um sistema grande e complexo**
  - **Identificação/documentação de propriedades fundamentais do sistema;**
  - **Correcção de inconsistências;**
  - **Possibilita desenhos alternativos do sistema.**
- **Processo de traduzir/interligar duas visões do mesmo sistema (Hardware view e Logical view).**
- **Métodos Formais têm poucos « clientes » no campo da Física de Altas Energias.**
- **Dissertação: especificação de uma nova componente (SMI* /SML) que será usada em todas as experiências do CERN que tenham um Sistema para Controlo de Detectores (DCS).**

* **SMI++ → State Management Interface (framework para a modelação e implementação de sistemas de controlo).**

Fim

Questão e Referências

Decomposição e Refinamento são dois elementos importantes no processo de desenvolvimento de software. Qual o papel dos métodos formais e suas ferramentas no desenho de sistemas complexos?

http://www.cern.ch/dsora/dsoraReport.pdf (relatório do projecto)
http://www.cern.ch
http://www.pvss.com

J. Fitzgerald, P. G. Larsen, P. Mukherjee, N. Plat and M. Verhoef. Validated Designs for Object-oriented Systems. Springer. 2005.

M. Verhoef. On the Use of VDM++ for Specifying Real-time Systems. Boderc project. Netherlands. 2000.

A. C. Balke, J. Carter, J. Haveman. Experience Using Formal Methods in High Energy Physics. CERN, Switzerland.1995.