FM&&T

Continuous Interaction in Safety Critical Systems

Mieke Massink

C.N.R.-ISTI, Pisa, Italy

—joint work with *Giorgio Faconti* (Pisa), *Gavin Doherty* (Pisa/CCRL) and the TACIT project —

F M&&T

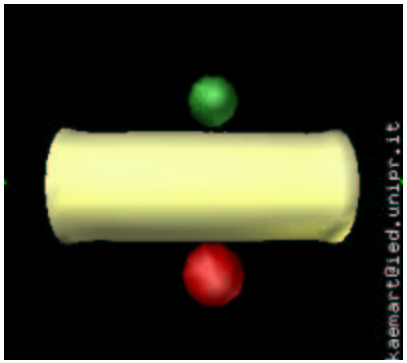
Overview

1. Introduction
2. Continuous Interaction
3. Aircraft Hydraulic Subsystem Interface
4. Magic Board Finger Tracking
5. Reference Model
6. Conclusions and Outlook

Examples of Continuous Interaction

- Virtual Piano
  CNR-ISTI ComputerArtLab

- Haptic Interaction
  Univ. of Parma, Ind. Engineering



- Magic Board
  IIHCM-Grenoble

- Hydraulic Subsystem
  Aircraft

Continuous Interaction in Future Computing Systems

F M&&T

Trends in HCI:

- Large number of non-standard devices
- Involving multiple senses simultaneously
- Invisibility of systems
- Ubiquity and mobility
- Virtual and intelligent environments

Design of Complex Concurrent Hybrid Systems

Consequences for system/interface design:

- Real-time, distributed, concurrent, mobile
- Cognitive requirements play a critical role

Interdisciplinarity:

- Engineering, Computer Science, Cognitive Psychology

Continuous vs. discrete interaction

Discrete interaction

- separate events (commands, mouse clicks)
- relatively short duration
- user controls progress

Continuous interaction

- series of information exchanges at high rate
- continuous perception
- progress is not only controlled by user
- reactive skills required
- (ICS terms: uninterupted cognitive configuration)

Continuity

Different definitions:

- Mathematically continuity is a property of **R**:

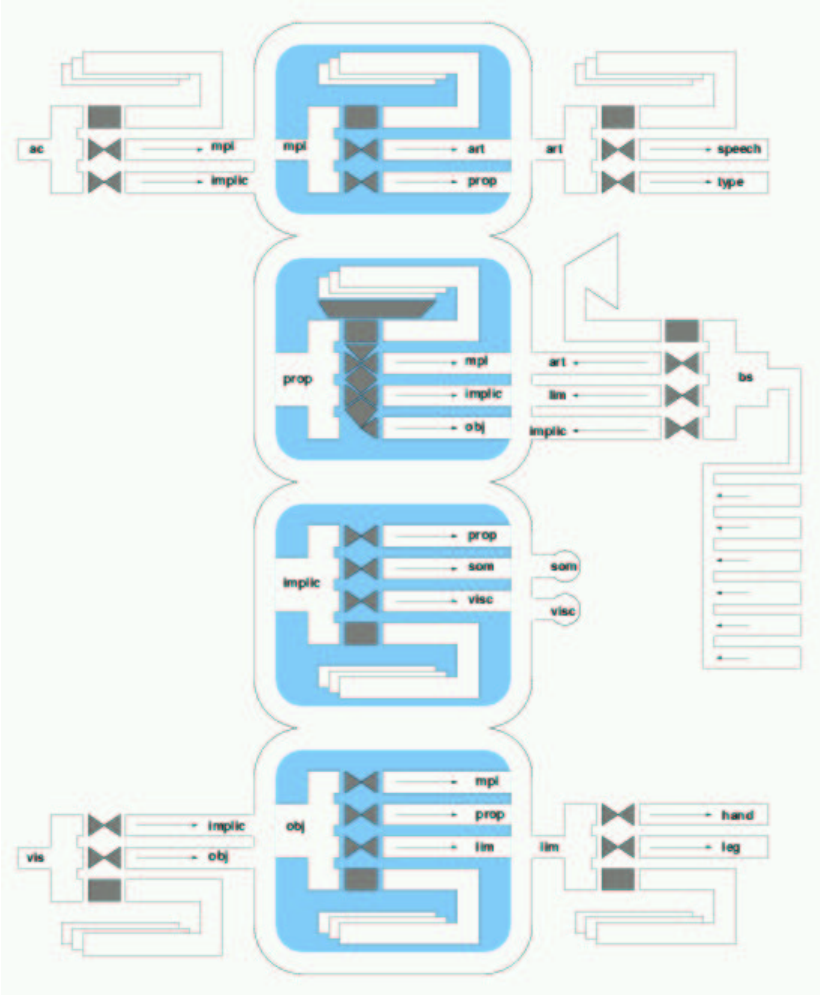
  Let a be a point in the domain of the function f(x). Then f is continuous at x=a if and only if

  $$\lim_{x \to a} f(x) = f(a)$$

  A function f(x) is continuous on a set if it is continuous at every point of the set. Finally, f(x) is continuous (without further modification) if it is continuous at every point of its domain.

- Cognitive Psychology:
  A configuration of a set of mental processes that is stable over an interval of time (ICS)

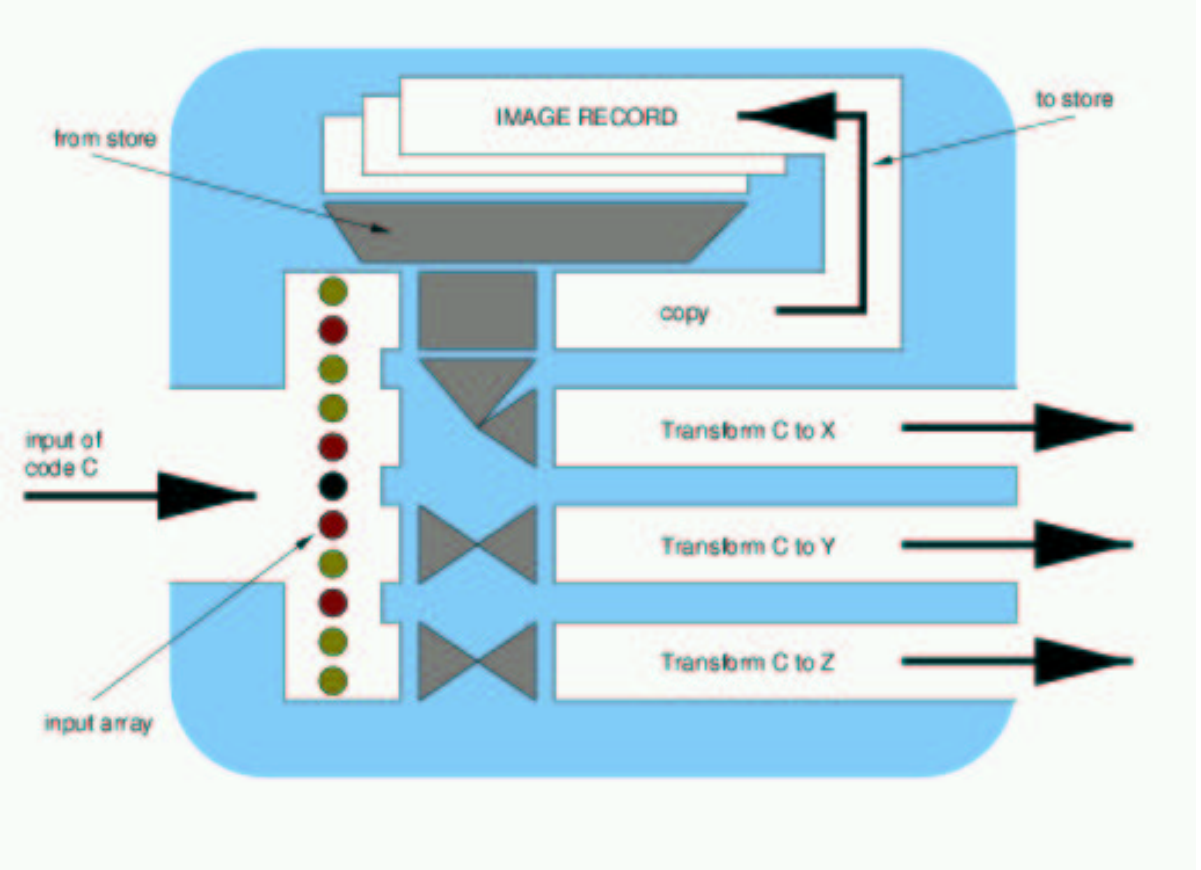
Interacting Cognitive Subsystems [Barnard]



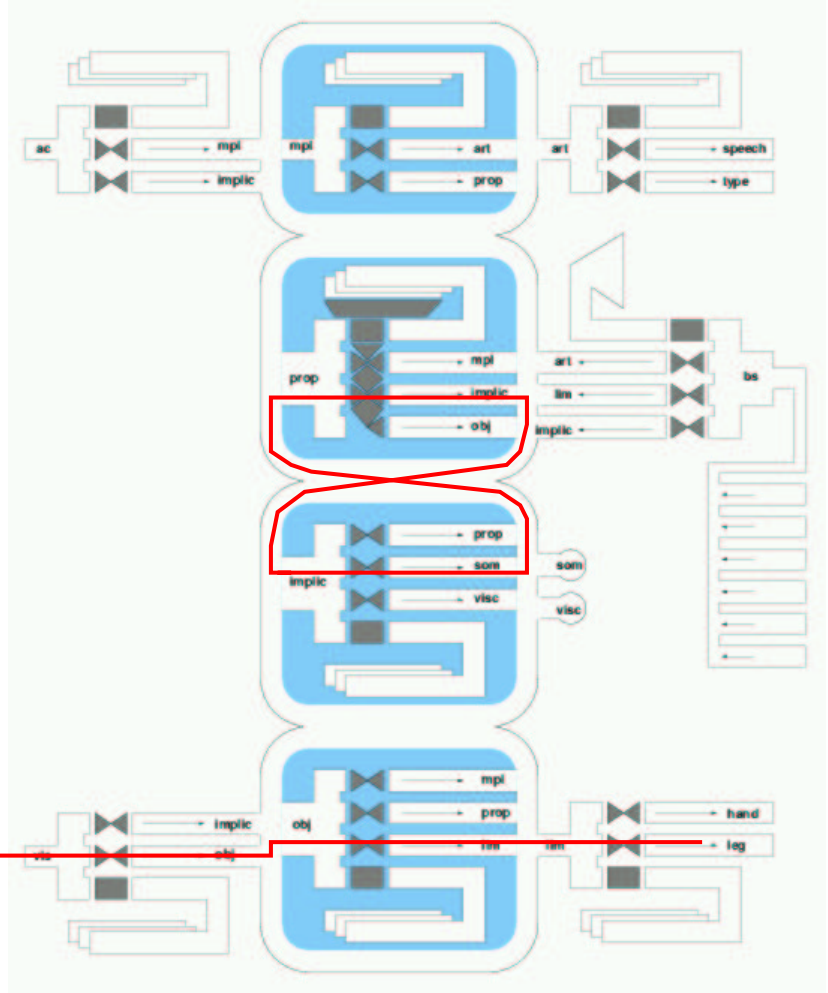
ICS assumes 9 subsystems:

- Sensory subsystems
  - VIS visual (eyes)
  - AC acoustic (ears)
  - BS body-state
- Effector subsystems
  - ART articulatory
  - LIM limb
- Structural subsystems
  - OBJ object
  - MPL morpholexical
- Meaning Subsystems
  - PROP propositional
  - IMPLIC Implicational

ICS Basic Unit of Information Processing



ICS Simultaneous activities



Simultaneous activities:

- Thinking
- Walking

Competing resources:

- Thinking
- Listening

Manual Control Theory

Use of continuous mathematics to model human performance

- anthropomorphic models
- optimal control approach

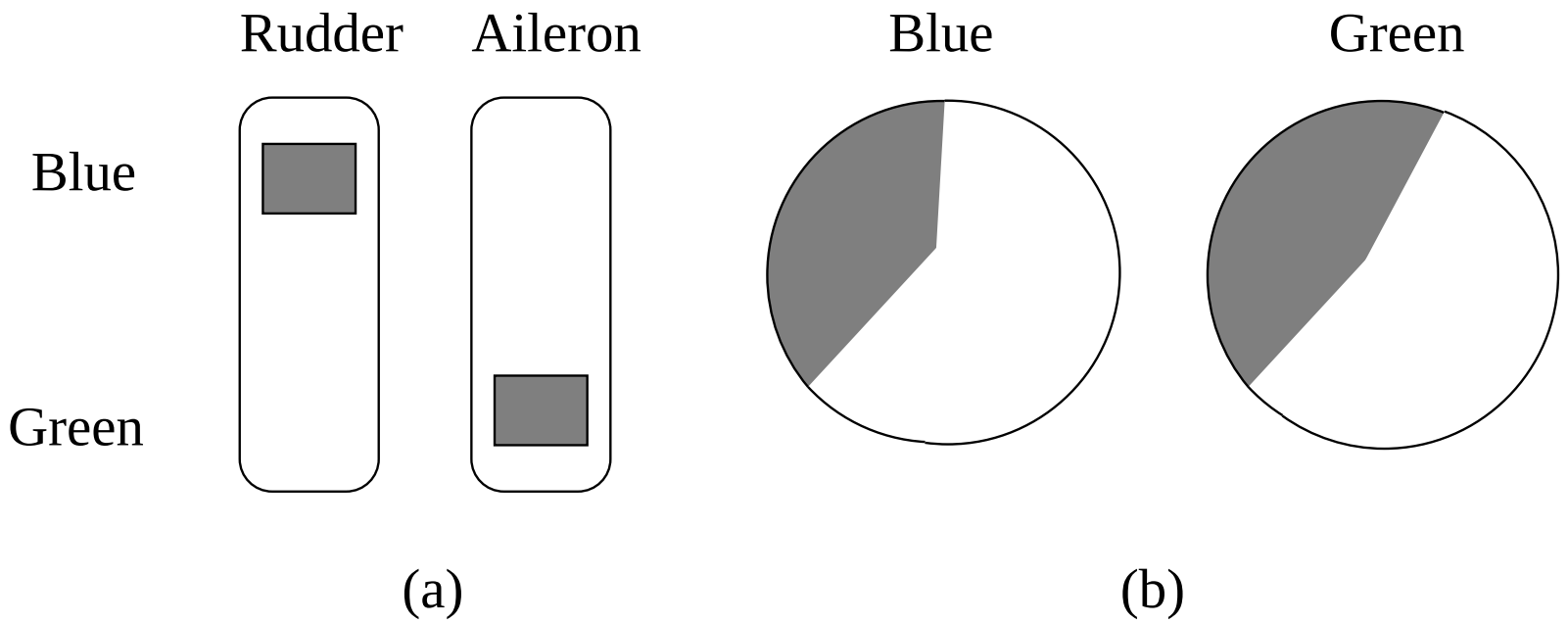
Classic types of systems:

- compensatory
- pursuit systems

Modern interfaces often have a mix of continuous and discrete tasks.

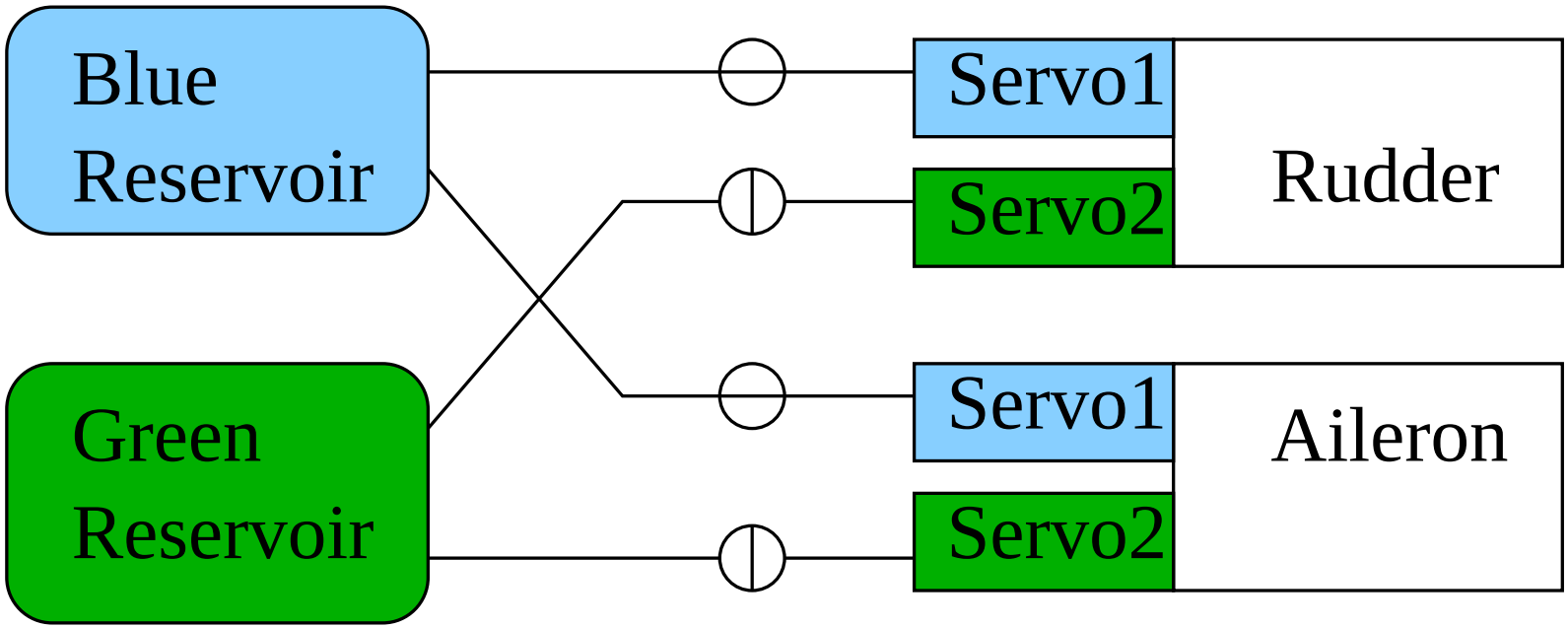
Hybrid Interfaces

Display of Aircraft Hydraulic Subsystem



Hybrid Interfaces:
Interfaces that contain both discrete and continuous components.

Simplified Aircraft Hydraulic Subsystem



Systematic Diagnosis and Repair

Diagnosis by active interaction with the system
Results of previous steps need to be remembered

Step	Control St.		Obs.		Possible causes of leak
	R	A	B	G	
1	B	B	L	N	$\neg\, GR \wedge (BR \vee R1 \vee A1)$
2	G	G	N	L	$\neg\, (BR \vee GR) \wedge (R1 \vee A1) \wedge (R2 \vee A2)$
3	B	G	L	L	$\neg\, (BR \vee GR) \wedge R1 \wedge A2$
4	G	B	N	N	$\neg\, (BR \vee GR \vee R2 \vee A1) \wedge R1 \wedge A2$

GR, BR: Green/Blue Reservoir
R1, R2: Rudder primary(blue)/secondary(green)
A1, A2: Aileron primary(blue)/secondary(green)

Order of steps is essential, history dependent

Conceptual/Task level analysis

Goal: Diagnosis and repair of hydraulic subsystem
Problem to diagnose: location of leaks in system
Repair actions: switching between reservoirs

Diagnosis:

- observe changes in level indicators
- relation between switch setting and indicator

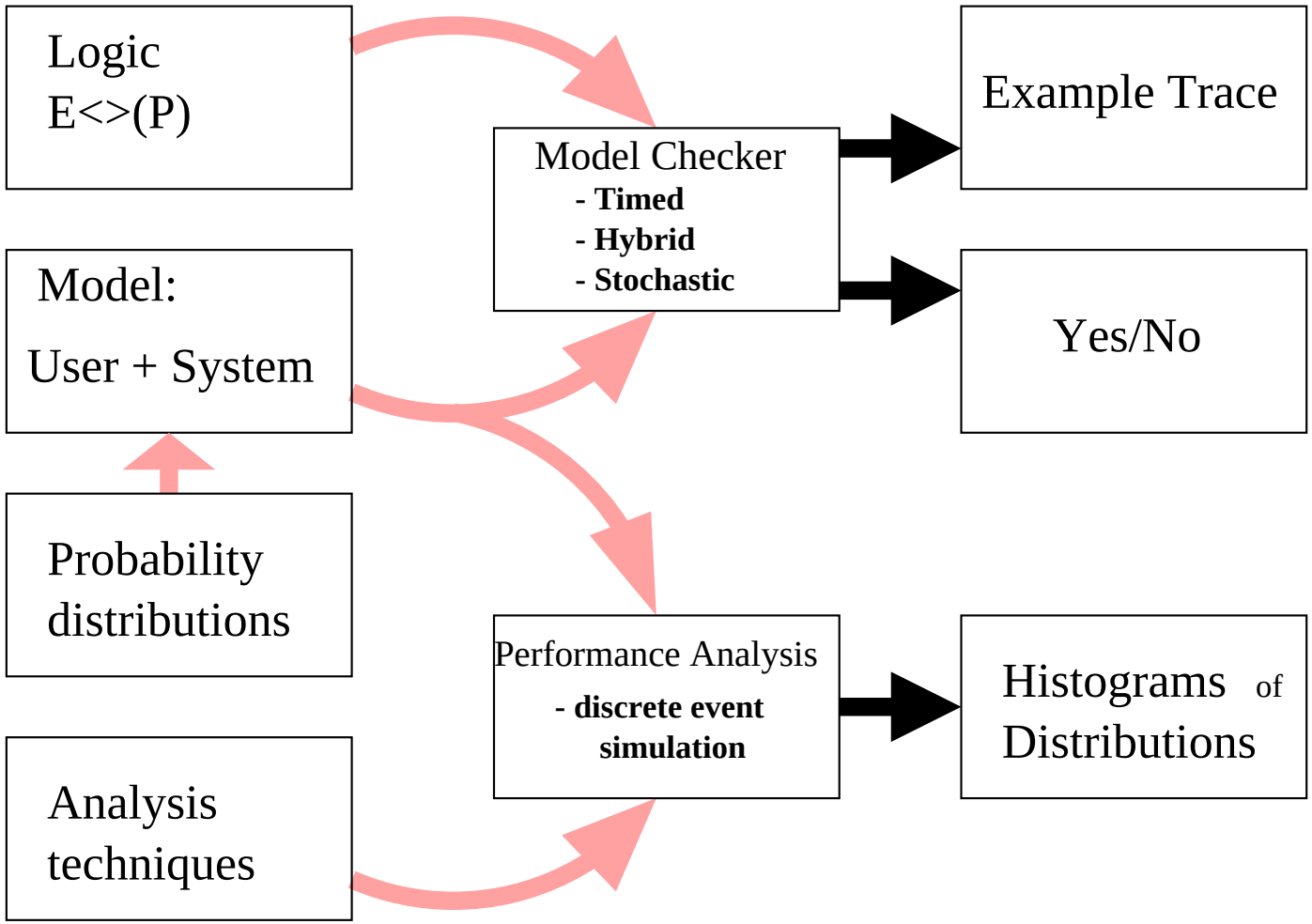
Correctness/completeness issues:

- Which combinations of leaks can be detected?
- Which combination of leaks can be repaired?

Performance issues:

- How much time does it take a pilot to perform fix/diagnosis?
- How much fluid would be lost/needed?
- Cognitive load?

Model Checking and Discrete Event Simulation



HyTech: Hybrid Systems Model Checker

FM&&T

Model checking tool for automatic verification of:
- real-time and hybrid system models
- modelled as sets of automata with linear differential equations

Developed at:
- Cornell University and Berkeley (1995).

Main people involved:
- Tom Henzinger
- Pei-Hsin Ho
- Howard Wong-Toi

Technique employed:
- Reachability analysis based on
- polyhedra technique to obtain a discrete representation of infinite state space

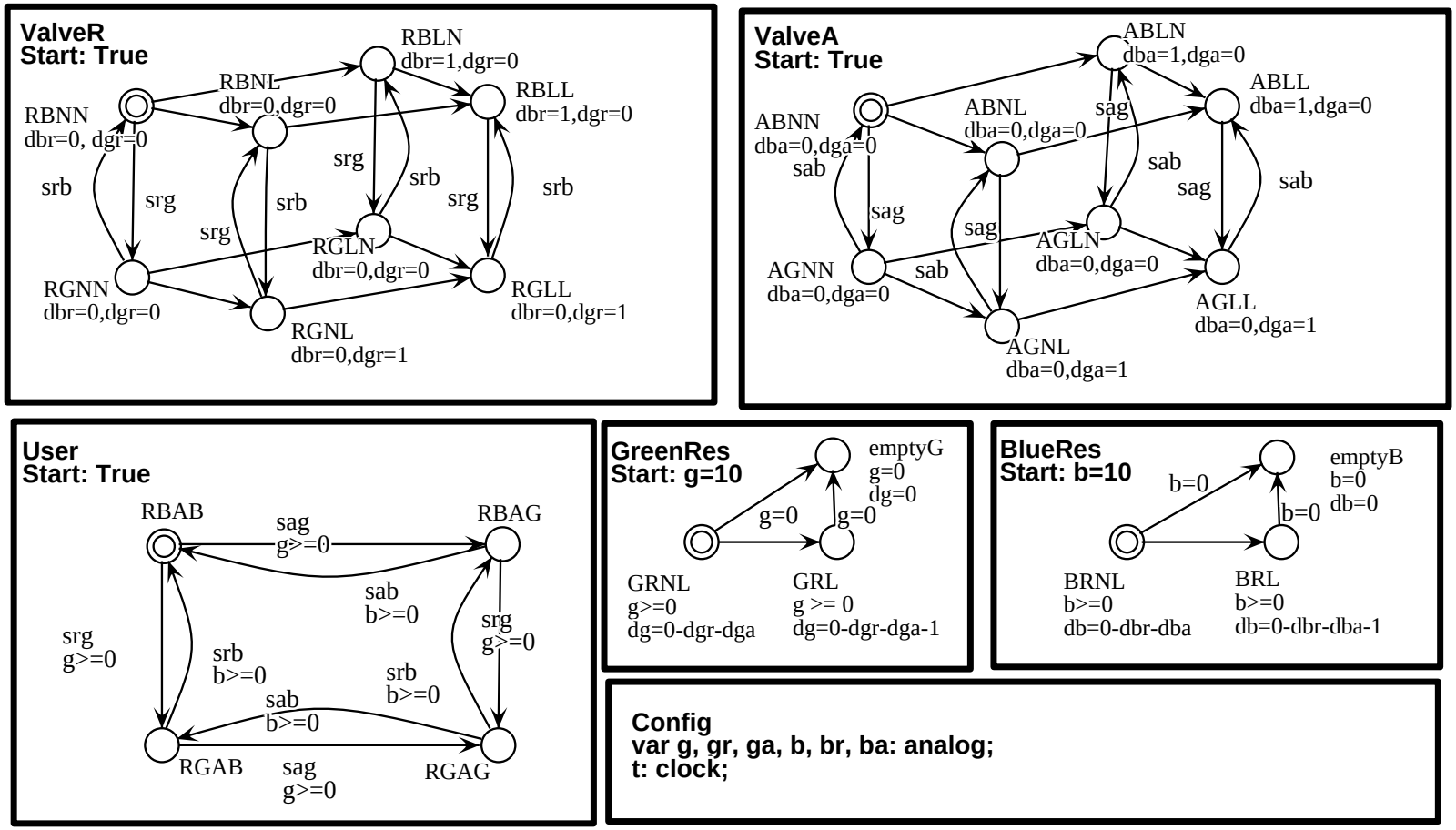
Hybrid Automata in HyTech

- Specification consists of a number of automata, variables and an analysis section
- Automata consists of locations linked by transitions
- Locations can have invariants and rate conditions
- Transitions have synchronisation labels, guards and variable assignments
- Variables can be discrete, clocks, stopwatches or analog
- Analysis by defining subsets of the state space and checking reachability between them

Syndetic Approach to Modelling

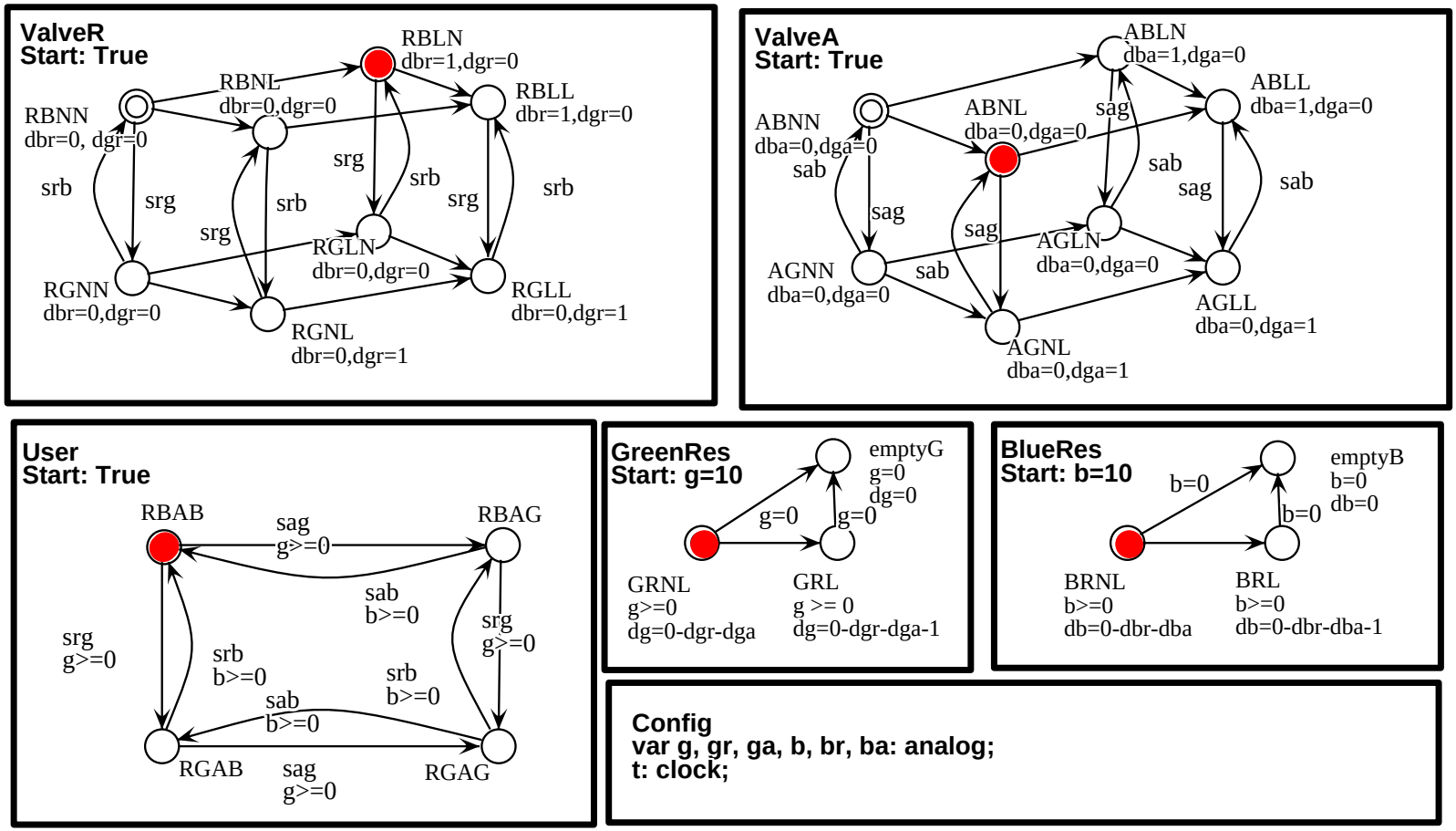
- Model aspects of both user and system
- Formal model of interface and formal model of cognitive resources needed to interact with devicesa
- Different (possibly simultaneous) activities involve several cognitive processes that may be in competition for concious attention and information
- User and system models linked by synchronised transitions and shared variables
- Semantic issues regarding interpretation of such links

Hybrid Automata Model



Reachability Analysis: Initial Region

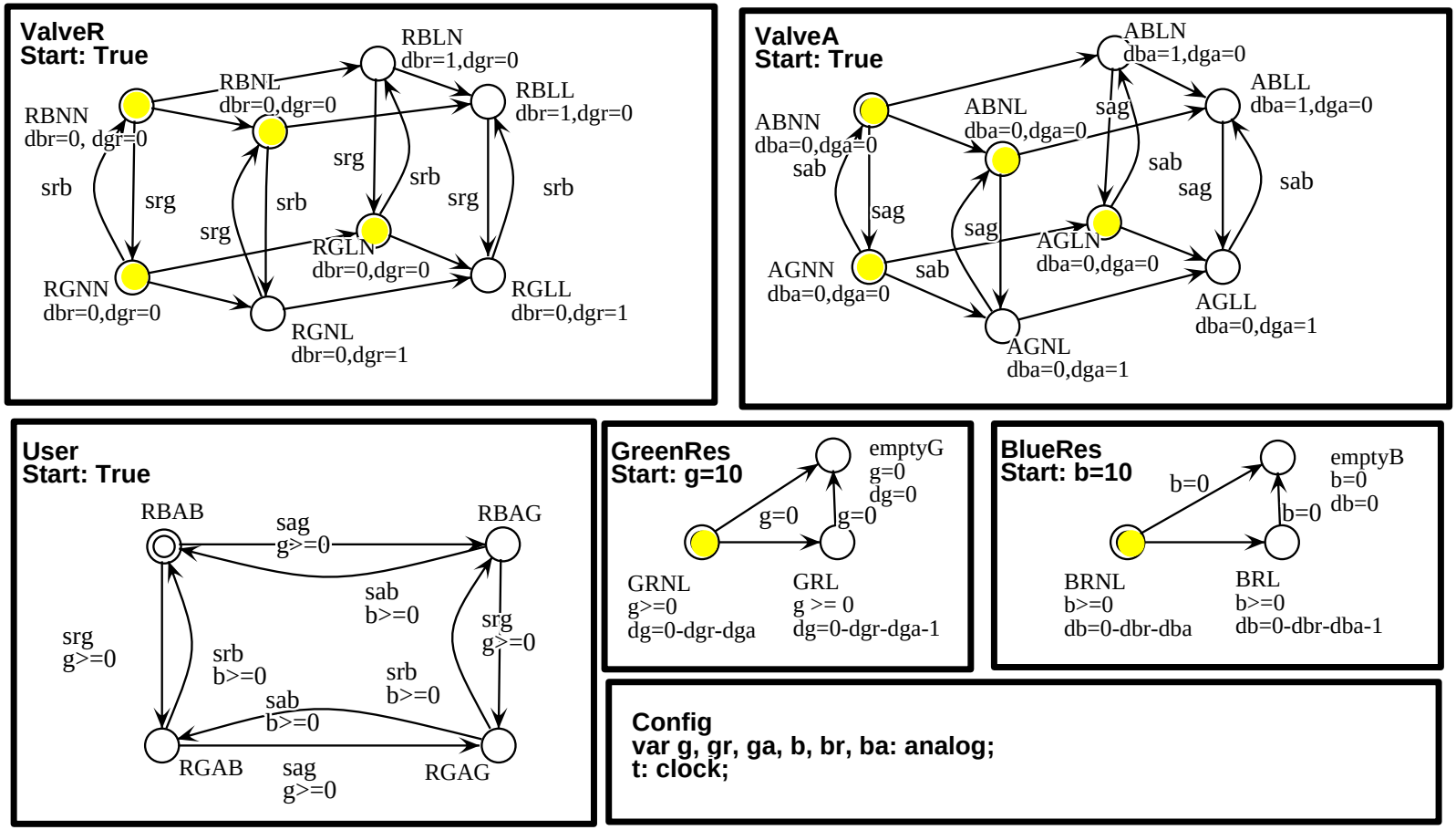
Initial Region characterises leaking situation:



Blue valve of rudder and green valve of aileron leaking Valves both on blue reservoir

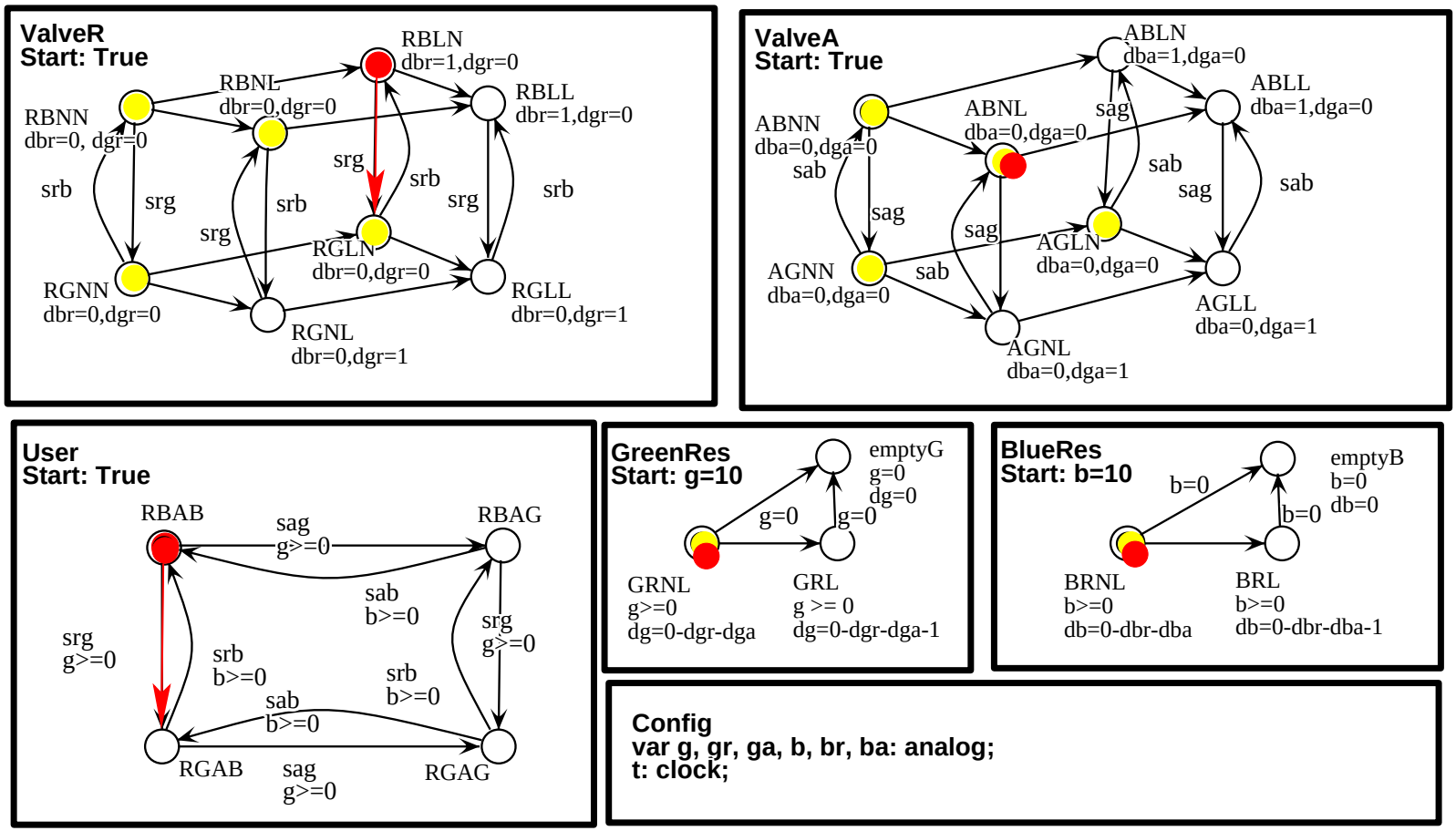
Reachability Analysis: Final Region

Final Region characterises non-leaking (non-empty) situation:



Forward reachability ∩ Final Region: move rudder to green

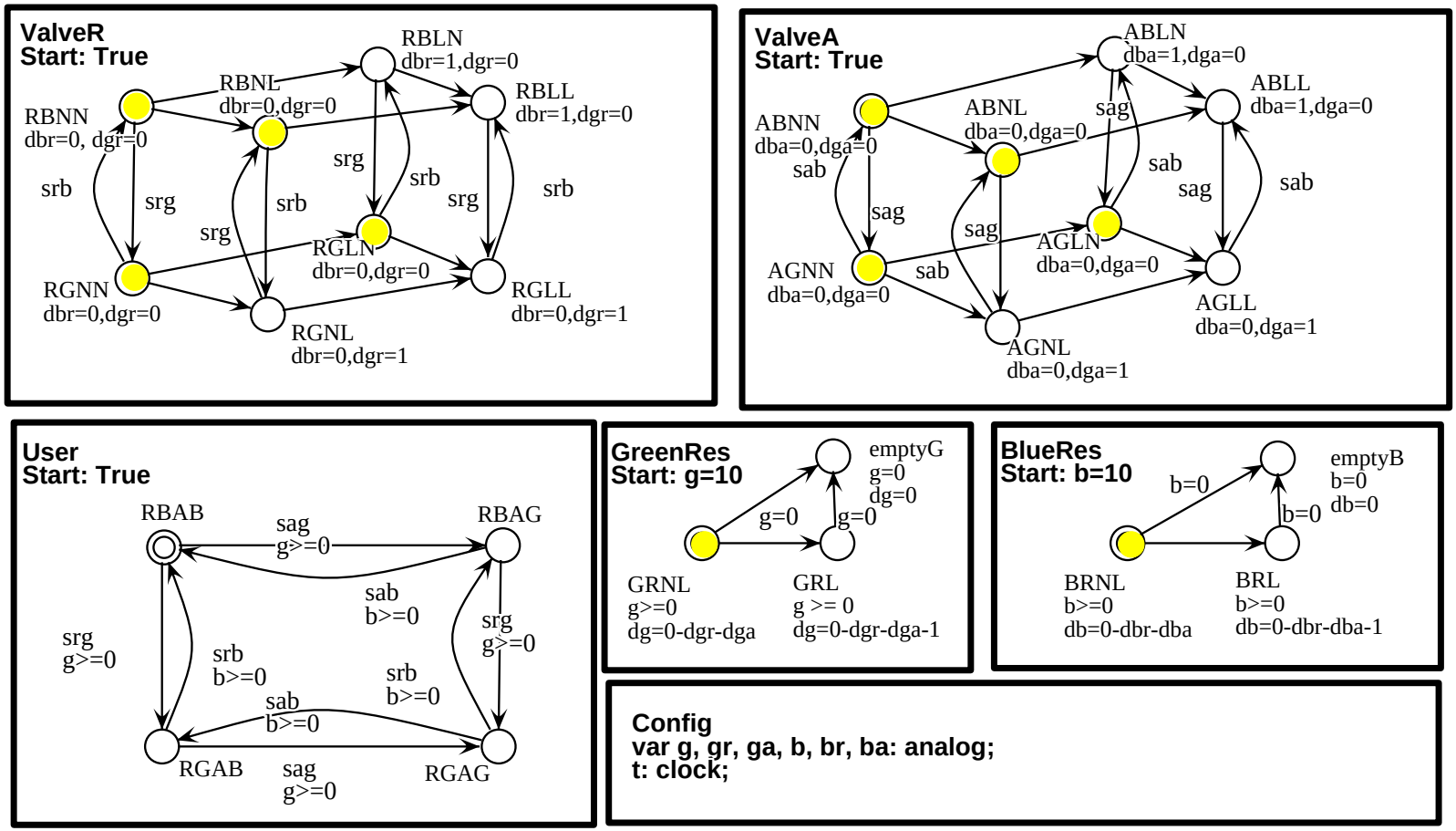
Reachability Analysis: Fixing Leak



Intersection forward reachable set s1 with Final Region gives possible solutions: User moves rudder to secondary (green) reservoir

Which leaks can be fixed?
Backward Reachability

Final Region characterises non-leaking (non-empty) situation:



Reservoirs not leaking and not both valves of any control surface are leaking at the same time.

Modelling Diagnosis and Repair

Diagnosis by active interaction with the system
Results of previous steps need to be remembered

Situation	Control St.		Obs.		Reachable situations
	R	A	B	G	
1	B	B	L	N	$s1$ = forward reach from sit1
2	G	G	N	L	$s2$ = forward reach from $s1$ & sit2
3	B	G	L	L	$s3$ = forward reach from $s2$ & sit3
4	G	B	N	N	$s4$ = forward reach from $s3$ & sit4

Size of s_i is indication for cognitive load (number of possibilities)
Unique result corresponds to complete fix/diagnosis
Hidden assumption in Field&Merriam: no further leaks during analysis

Analysis results

Exactly which ‘leaky’ situations can the pilot fix with the given interface?

Search ‘backwards’ from ‘no-leak’ situation:
Both reservoirs are *not* leaking AND
never *both* valves of same control surface are leaking

Which repair and diagnosis strategies would be most efficient?
Differences in time to fix problem
Differences in memory load and reasoning
Differences in information vs. repair

Given reasoning capabilities of pilot and likely bounds on leaks:
What would be a safe amount of liquid?

Stochastic Models of Interaction

User behaviour is typically stochastic:
it is neither deterministic
nor completely random

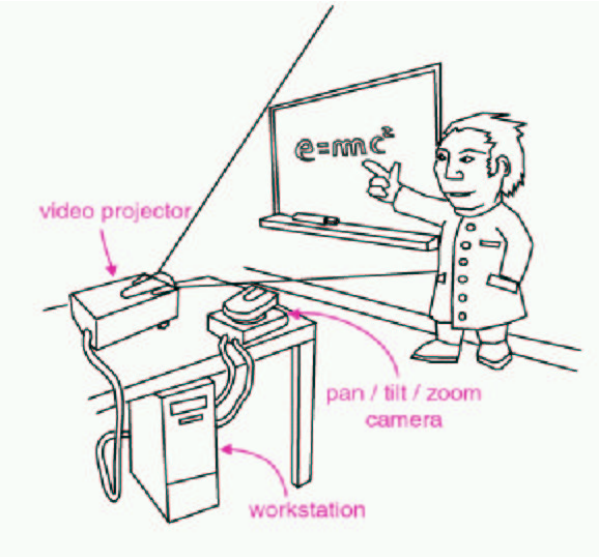
Human behaviour follows a certain probability distribution

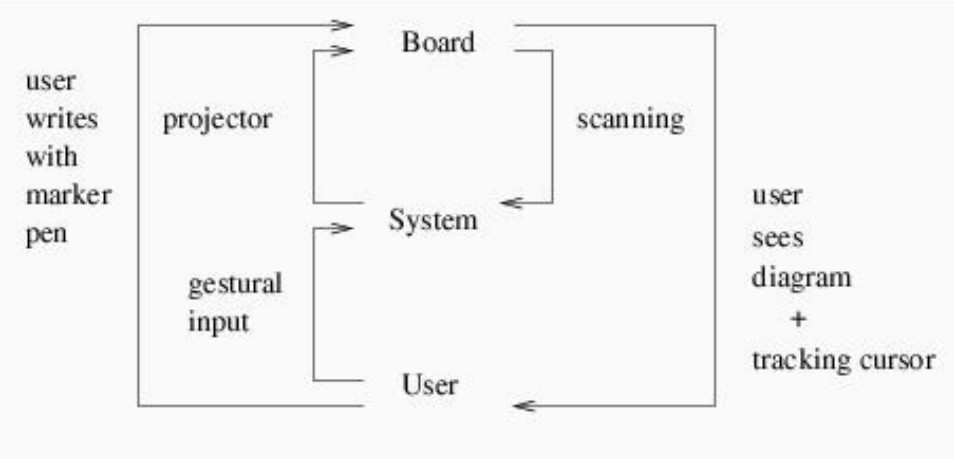
Stochastic modelling attempts to forecast
combined human-system performance.

Stochastic variables in human performance:
- Performance w.r.t. *time*
- Performance w.r.t. *errors*

Finger Tracking on Magic Board

How accurate/fast should the cursor follow the finger?





Fitts' Law:

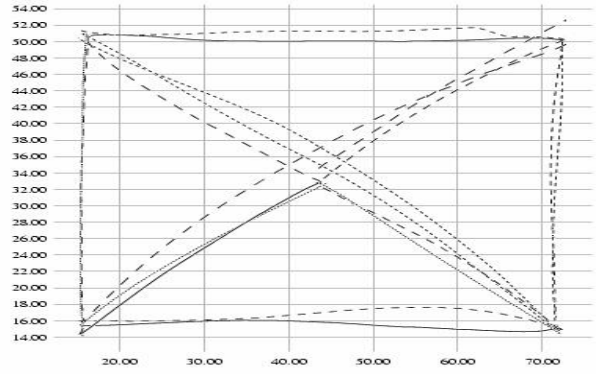
$$MT = a + b \log 2(2A/W)$$

MT = movement time a,b = regression coefficients

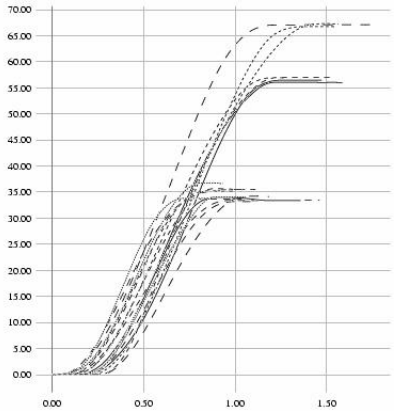
A = distance of movement from start to target center

W = width of the target

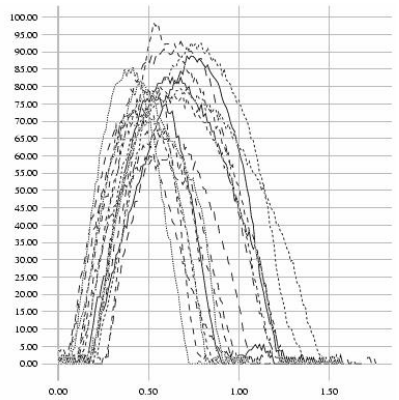
Experimental Results Pointing on Whiteboard



XY movements

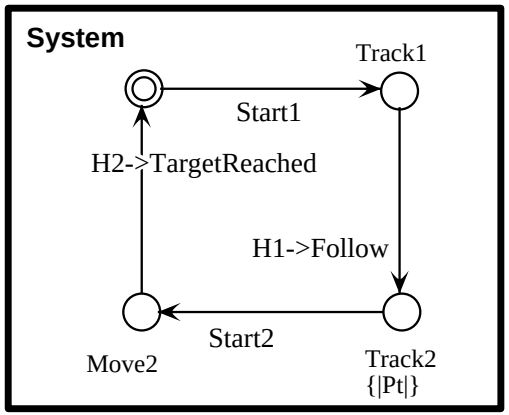


Distance vs time

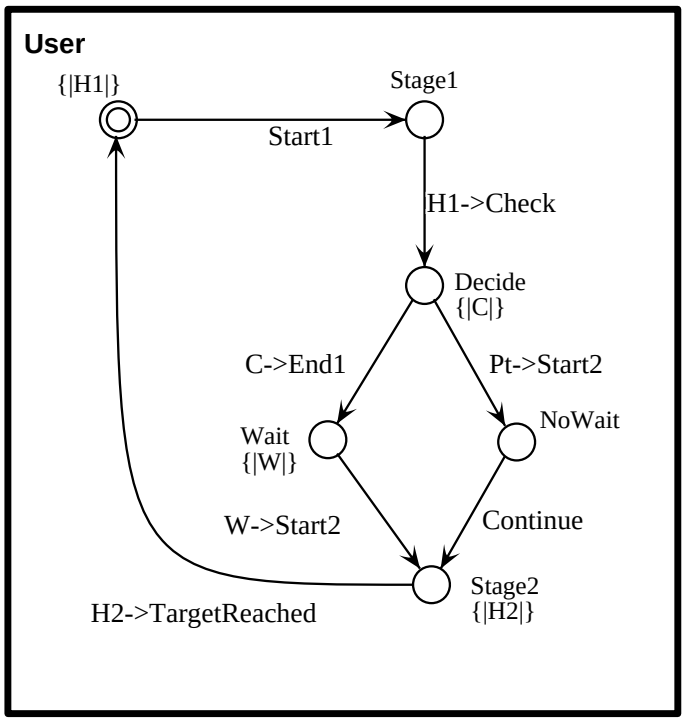


Velocity vs time

Stochastic Model Finger Tracking

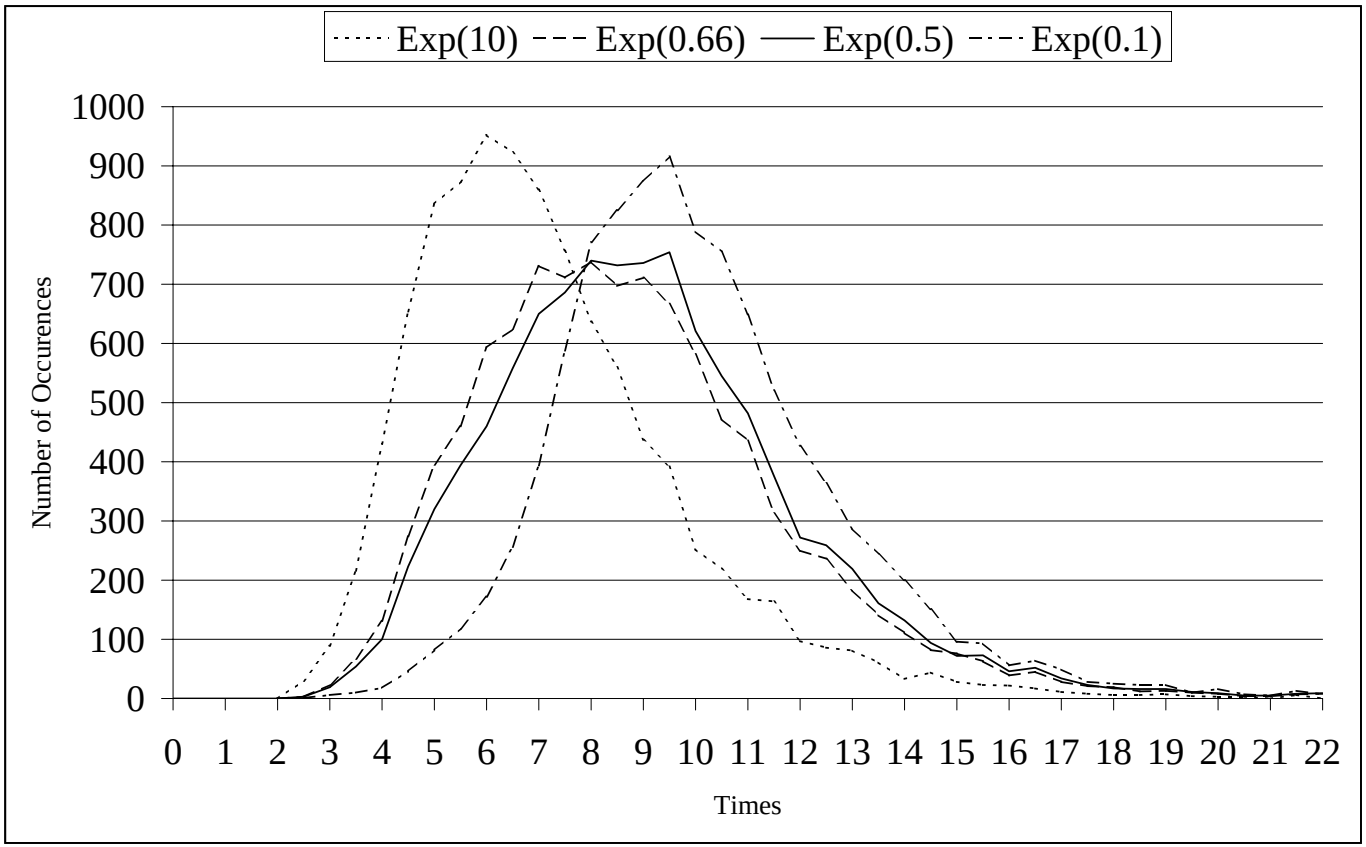


Clocks Pt: Exp(1.0)
H1: Lognorm(2.3 1.4)
H2: Lognorm(4.4 1.6)
C: Unif(0.25 1.7)
W: Unif(0.55 2.7)
System
||{Start1, Start2, TargetReached}
User



Results Stochastic Model

Bimodal distribution between $\lambda = 1.5$ and $\lambda = 0.5$
Corresponding to system average delay of 60 to 200 ms.



Time in ms $*$ 10

Layered Approach to Scientific Abstraction

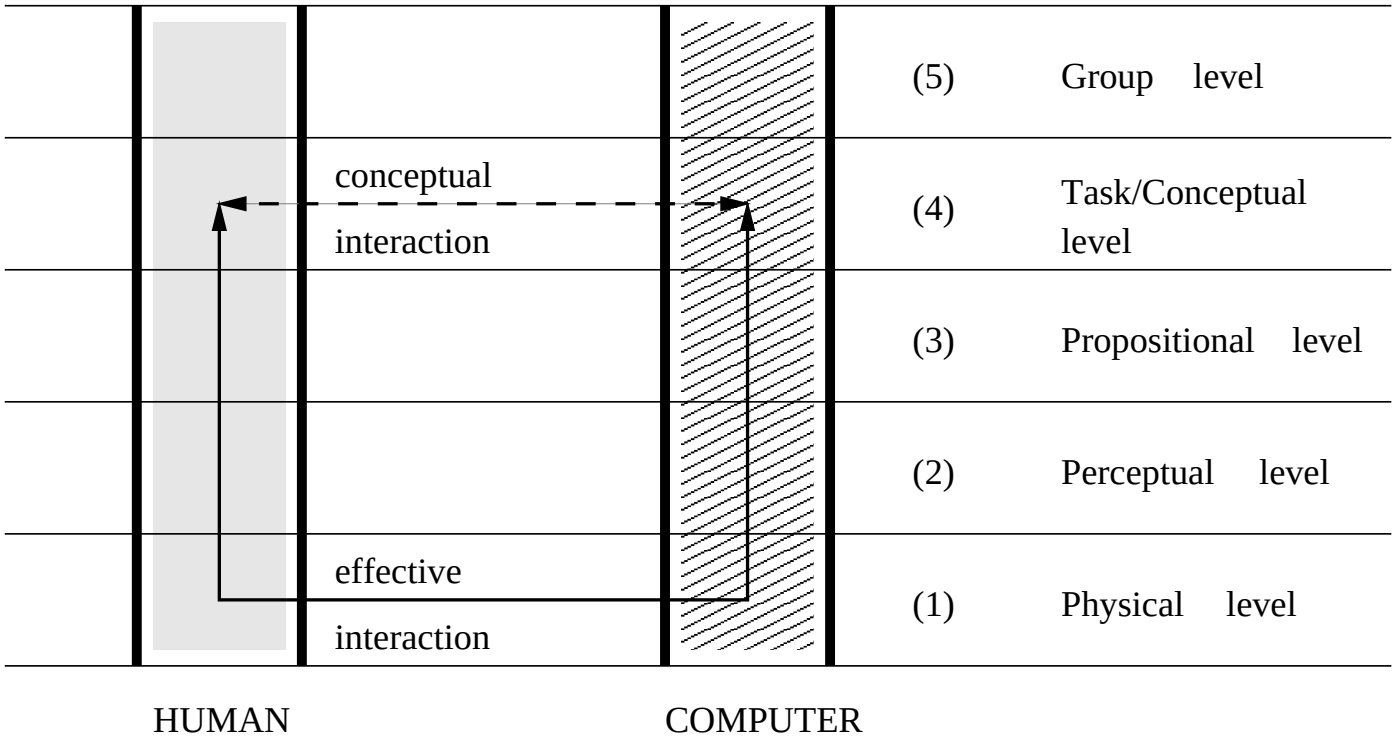
Interdisciplinary theories:
- Systems, Interactions and Macrotheory[Barnard et al.99]

Theories of Interaction:
- Skill-Rule-Knowledge Model [Rasmussen 1980]
- Seven Stage Model [Norman 1990]

Communication protocols:
- Reference Model for Network Protocols [Zimmermann ISO-ISO 1980]

Continuous Interaction:
- Reference Model for Continuous Interaction

Reference model for Continuous Interaction



Conclusions and Issues

- Formal model checking approach to hybrid interfaces
- Human behaviour is inherently variable
  Instead of disregarding this, better to consider it
- Stochastic model based approaches seem promising
- Difficulty: obtain reliable information for model
- Many aspects of human behaviour not known/very variable
- Training/learning aspects

F M&&T

Acknowledgements

This work is being supported by the European Commission under contract ERB FMRX CT97 0133 - TACIT (Theory and Applications of Continuous Interaction Techniques).

Partners: Istituto CNUCE, IT (coordinator)
CRLC - RAL, UK
DFKI, GE
FORTH, GR
University of Bath, UK
University J.Fourier, FR
University of Parma, IT
University of Sheffield, UK
University of York, UK

http://kazan.cnuce.cnr.it/TACIT/TACIThome.html