State Event Models for the Formal Analysis of Human-Machine Interactions

Sébastien Combéfis[1] Dimitra Giannakopoulou[2]
Charles Pecheur[1]

[1]Université catholique de Louvain (UCL)
ICT, Electronics and Applied Mathematics Institute (ICTEAM)

[2]NASA Ames Research Center (ARC)

March 26, 2014

UCL
Université
catholique
de Louvain

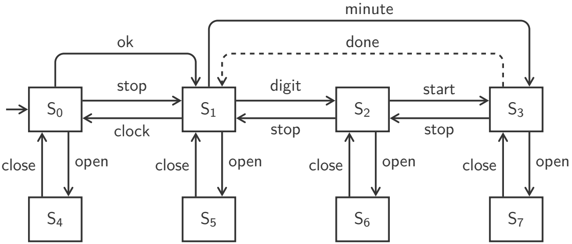
[FVHMS 2014, Palo Alto, USA]

Introduction

- Automated formal analysis techniques for HMI systems
- Detection of potential automation surprises
- Conformance relation between actual system and mental model according to which it is operated

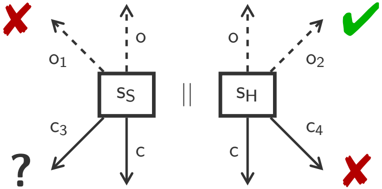
Formal Modelling

- HMI-LTS extends LTS with inputs and outputs:
  - Commands executed by the user
  - Observations executed by the system and observed by the user
  - Internal actions invisible to the user



Interaction Model

- **Interaction:**
  - Represented with the synchronous parallel composition



- **Bad situations:**
  - A command missing on the system model (c_4)
  - An observation missing on the mental model (o_1)

Full-control property

- Full-control property captures safe interaction

- During the interaction between a user and a system:
  - The user must know exactly the possible commands...
  - ...and at least all the possible observations

$\mathcal{H}\,\mathrm{fc}\,\mathcal{S}$ if and only if :

$$\forall \sigma \in \mathcal{L}^* \text{ such that } s_S \in (s_{0_S}\ \textbf{after}\ \sigma) \text{ and } s_H \in (s_{0_H}\ \textbf{after}\ \sigma) :$$

$$A^c(s_S) = A^c(s_H) \quad \text{and} \quad A^o(s_S) \subseteq A^o(s_H)$$

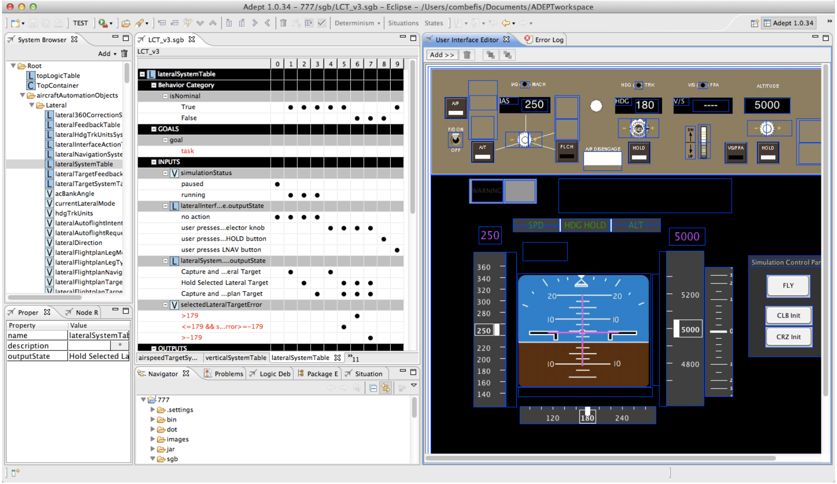
Generation Problem

- **Goal:** Given the model of a system, automatically generate a minimal full-control conceptual model
- **Motivation:**
  - Extract the minimal behaviour of the system, so that it can be controlled without surprise
  - Help to build artifacts: manuals, procedures, trainings, . . .
  - If such abstraction does not exist, provide feedback to help redesigning the system

ADEPT toolset

- Automatic Design and Evaluation Prototyping Toolset
- Java-based tool
- Support designers in early prototyping phases of automation interfaces

Autopilot ADEPT model I



Property	Value
name	lateralSystemTab
description	*
outputState	Hold Selected La

	0	1	2	3	4	5	6	7	8	9
lateralSystemTable										
Behavior Category										
isNominal										
True		●	●	●	●	●				●
False							●	●	●	
GOALS										
goal										
task										
INPUTS										
simulationStatus										
paused	●									
running		●	●	●						
lateralInterf...e.outputState										
no action	●	●	●	●						
user presses...elector knob					●	●	●	●		
user presses...HOLD button									●	
user presses LNAV button										●
lateralSystem....outputState										
Capture and ...eral Target		●			●					
Hold Selected Lateral Target			●			●	●	●		
Capture and ...plan Target				●		●	●	●		
selectedLateralTargetError										
>179							●			
<=179 && s...rror>=-179						●				
>-179								●		
OUTPUTS										

Autopilot ADEPT model II

	0	1
L airspeedFeedbackTable		
INPUTS		
L airspeedSystemTable.outputState		
Maintain Airspeed Target	●	
Capture Airspeed Target	●	
Hold Current Airspeed	●	
Protect Airspeed Target		●
OUTPUTS		
C pfdAirspeedTape.currentValue		
V indicatedAirspeed	●	●
C cautionLabel.background		
255, 204, 0		●
C autothrottleModeFailureBar.opaque		
False	●	
True		
C pitchModeFailureBar.opaque		
False	●	
True		
C pfdAirspeedTape.preSelectedTarget		
V selectedSpeedTarget		●
C pfdAirspeedTape.selectedTarget		
V selectedSpeedTarget		●

State Event Models

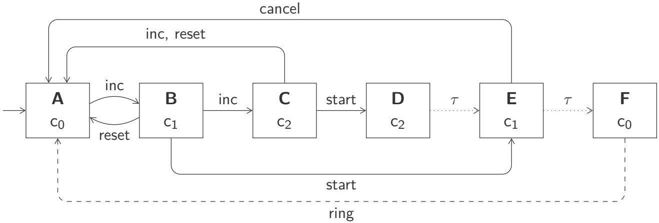
- ADEPT models combine state with transition information
- A state is made of n variables x_i ranging over domains D_i
- Only some state-variable are visible

$$\begin{tikzcd} \boxed{\langle x_1 = v_1, \ldots, x_n = v_n \rangle} \arrow[r] & \boxed{\langle x_1 = v'_1, \ldots, x_n = v'_n \rangle} \end{tikzcd}$$

HMI-LTS are enriched with state-values

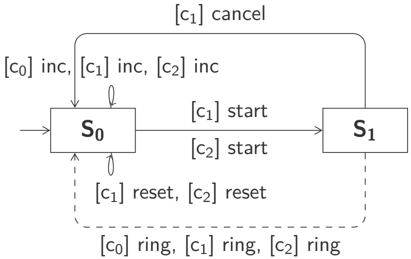
HMI State-Valued System Model

- Each state s is associated with a state-value $\mathcal{O}(s)$
- Two kinds of observations are possible in a system



HMI State-Valued Mental Model

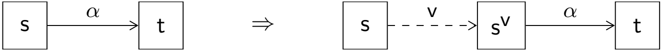
- Transition are guarded with a state-value
- A transition will be executed if the guard is satisfied in the current state of the system



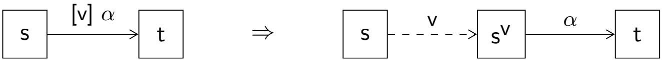
[c_1] cancel
[c_0] inc, [c_1] inc, [c_2] inc
[c_1] start
$\mathbf{S_0}$
$\mathbf{S_1}$
[c_2] start
[c_1] reset, [c_2] reset
[c_0] ring, [c_1] ring, [c_2] ring

Enriched models to HMI-LTS

- System model



- Mental model



- The transformation preserves the developed algorithms

Conclusion

- An enriched model for system and mental model
- Translation from ADEPT models (to be automated)
- Reverse translation from HMI-LTS to ADEPT to be done