Formal Analysis of Human-Automation Interaction

Sébastien Combéfis

Computer Science and Engineering Department (INGI)
Louvain School of Engineering (EPL)
Université catholique de Louvain, Belgium (UCL)

June 24, 2008

[MOVEP'08]

Outline

Outline

The problem

What ? Analyzing interaction between human and machine

Why ? Accidents due to bad interaction : Therac-25, KAL007, Royal Majesty cruise ship, . . .

How ? Using formal methods to analyze and reason about such interactions (Rushby, Degani)

The problem

What ? Analyzing interaction between human and machine

Why ? Accidents due to bad interaction : Therac-25, KAL007, Royal Majesty cruise ship, . . .

How ? Using formal methods to analyze and reason about such interactions (Rushby, Degani)

The problem

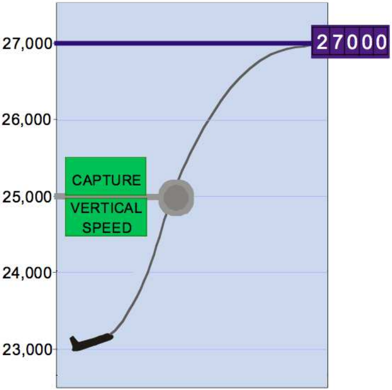
What ? Analyzing interaction between human and machine

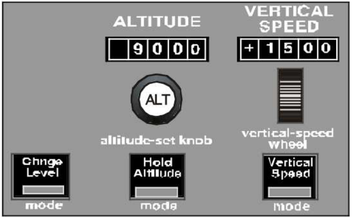
Why ? Accidents due to bad interaction : Therac-25, KAL007, Royal Majesty cruise ship, ...

How ? Using formal methods to analyze and reason about such interactions (Rushby, Degani)

The problem

An example (Rushby)

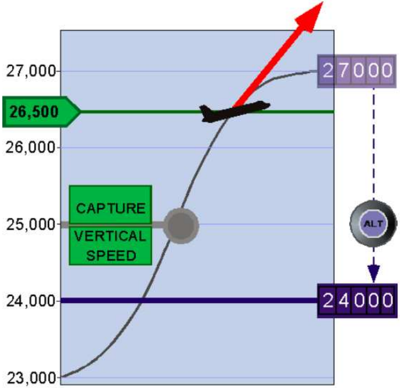


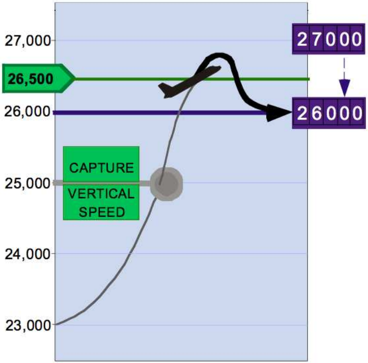


Guidance Control Panel

The problem

An example (Rushby)





The problem

Summary

- A user have to operate a machine
- He has a certain knowledge about the machine
- The machine is partially controllable and observable

Outline

Formalization

Modelling

Machine model $M = \langle S_M, \mathcal{L}_M, \rightarrow_M, s_{0_M} \rangle$

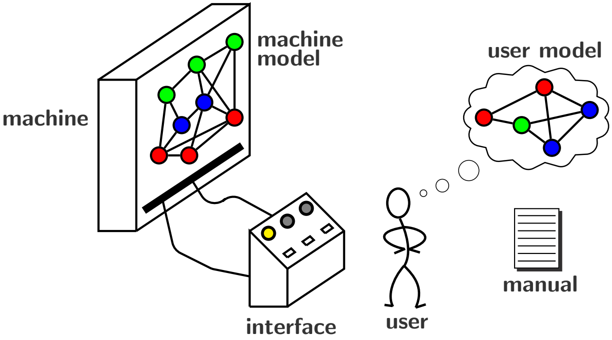
$\mathcal{P}_M = \{P_1, \cdots, P_k\}$, partition of S_M (modes)

$\mathcal{L}_M = \mathcal{L}_M^c \uplus \mathcal{L}_M^o \uplus \{\tau\}$, three kind of actions

User model $U = \langle S_U, \mathcal{L}_U, \rightarrow_U, s_{0_U} \rangle$

Formalization

Addressed problem



Formalization

Addressed problem

- Given a machine model, synthetize a user model
- The user model is an abstraction of the machine model
- The user must know the current mode of the machine and the next mode in response to an action

Formalization

Synthesis of reduced model

- Coarsest refinement of $\mathcal{P}_M$ with respect to an equivalence $\sim_{\text{red}}$

  User model given by the quotient $S_U = S_M / \sim_{\text{red}}$

- $s \sim_{\text{red}} s' \implies [s]_{\mathcal{P}_M} = [s']_{\mathcal{P}_M}$

Formalization

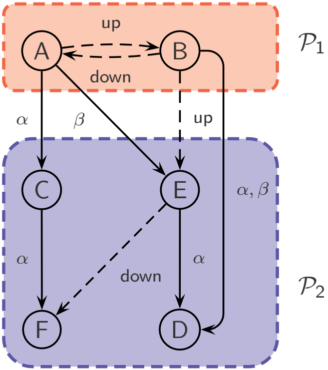
Equivalence definition (I)

1. $s \sim_{\text{red}} s' \iff A^c(s) = A^c(s') \wedge$
   $\forall s \xrightarrow{\alpha \in A^c(s)} t, s' \xrightarrow{\alpha} t' : [t]_{\mathcal{P}_M} = [t']_{\mathcal{P}_M}$

2. $s \sim_{\text{red}} s' \iff \forall s \xrightarrow{\alpha \in \mathcal{L}_M^c} t : \exists s' \xrightarrow{\alpha} t' : t \sim_{\text{red}} t' \wedge$
   $\forall s' \xrightarrow{\alpha \in \mathcal{L}_M^c} t' : \exists s \xrightarrow{\alpha} t : t \sim_{\text{red}} t' \wedge$
   $\forall s \xrightarrow{\alpha \in \mathcal{L}_M^o} t : \exists s' \xrightarrow{\alpha} t' \implies t \sim_{\text{red}} t' \wedge$
   $\forall s' \xrightarrow{\alpha \in \mathcal{L}_M^o} t' : \exists s \xrightarrow{\alpha} t \implies t \sim_{\text{red}} t'$

Example

Equivalence definition (I)



Formalization

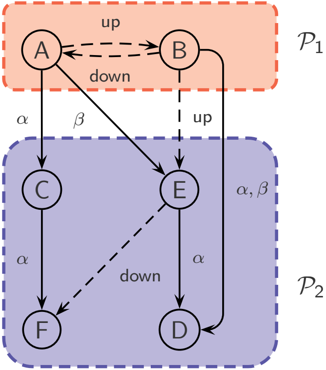
Equivalence definition (II)

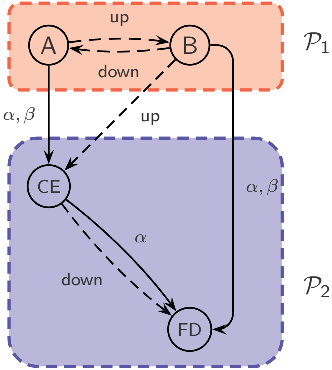
1. $s \sim_{red} s' \quad \Leftrightarrow \quad A^c(s) = A^c(s') \wedge$
   $\forall s \xrightarrow{\alpha \in A^c(s)} t, s' \xrightarrow{\alpha} t' : [t]_{\mathcal{P}_M} = [t']_{\mathcal{P}_M}$

2. $s \sim_{red} s' \quad \Leftrightarrow \quad \forall s \xrightarrow{\alpha \in \mathcal{L}^c_M} t : \exists s' \xrightarrow{\alpha} t' : t \sim_{red} t' \wedge$
   $\forall s' \xrightarrow{\alpha \in \mathcal{L}^c_M} t' : \exists s \xrightarrow{\alpha} t : t \sim_{red} t' \wedge$
   $\forall s \xrightarrow{\alpha \in \mathcal{L}^o_M} t : \exists s' \xrightarrow{\alpha} t' \implies t \sim_{red} t' \wedge$
   $\forall s' \xrightarrow{\alpha \in \mathcal{L}^o_M} t' : \exists s \xrightarrow{\alpha} t \implies t \sim_{red} t'$

Example

Equivalence definition (II)





Outline

Ongoing work

- Taking into account internal action (τ)
- Testing and evaluating equivalences on some real examples
- Formalizing relations between
  machine model – user interface – user model
- Exploring works on bisimulation, diagnosability, control theory, . . . (Any ideas or suggestions on any relevant work are welcome)

Questions

Thank you for your attention

Questions ?

Sébastien Combéfis

Sebastien.Combefis@uclouvain.be