Formal Verification of Human-Automation Interaction

Asaf Degani, Michael Heymann

ParaDiSe Seminar, spring 2008

April 14, 2008

The Problem

- Advanced automation brings unexpected problems.
- Deficiencies in human computer interaction
- Advanced automation systems: Automatic Flight Control Systems (AFCS)

Example

On climb to 27,000 feet and leaving 26,500 feet. Memphis Center gave us a clearance to descend to 24,000 feet. The aircraft had gone to "Capture" mode when the first officer selected 24,000 feet on the GCP altitude setting. This disarmed the altitude capture and the aircraft continued to climb at approximately 300 feet-per-minute. There was no altitude warning and this "altitude bust" went unnoticed by myself and the first officer, due to the slight rate-of-climb. At 28,500, Memphis Center asked our altitude and I replied 28,500 and started an immediate descent to 24,000 feet.

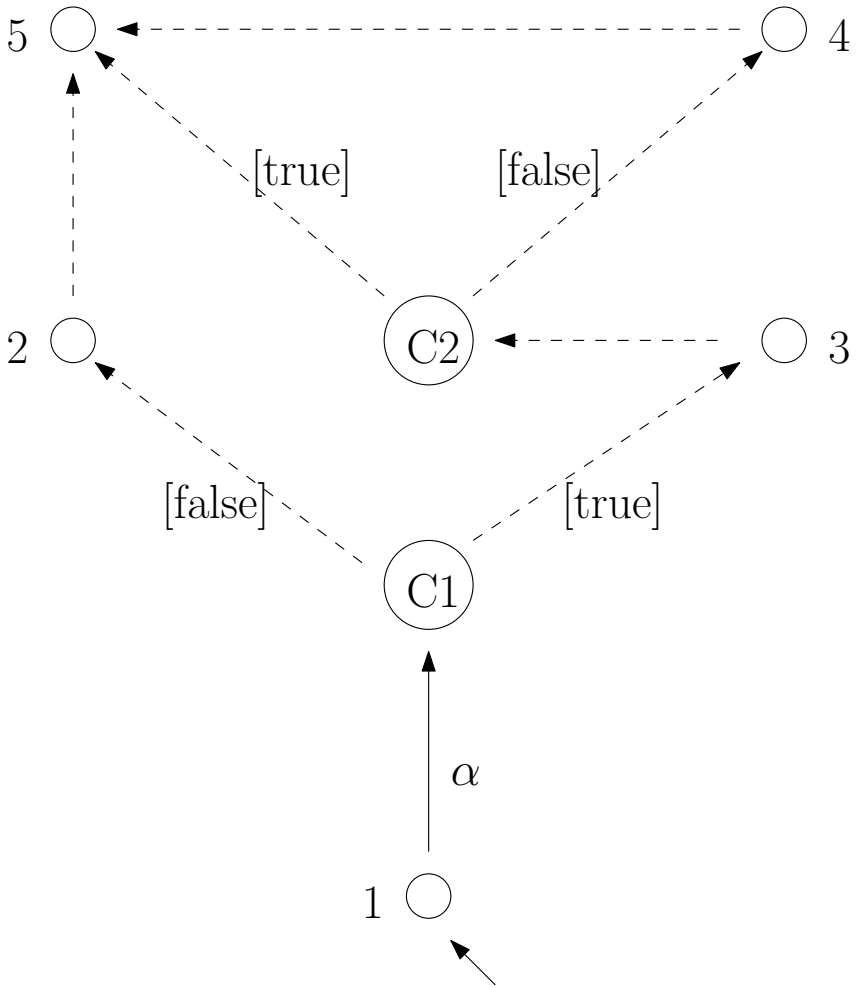
Human Machine Interaction

- Machine's behavior
- The task specification
- The user-model
- The user interface

Assumptions

- Machine's behavior modeled formally
- Machine's behavior deterministic
- The task specification specified
- The user's knowledge formally represented

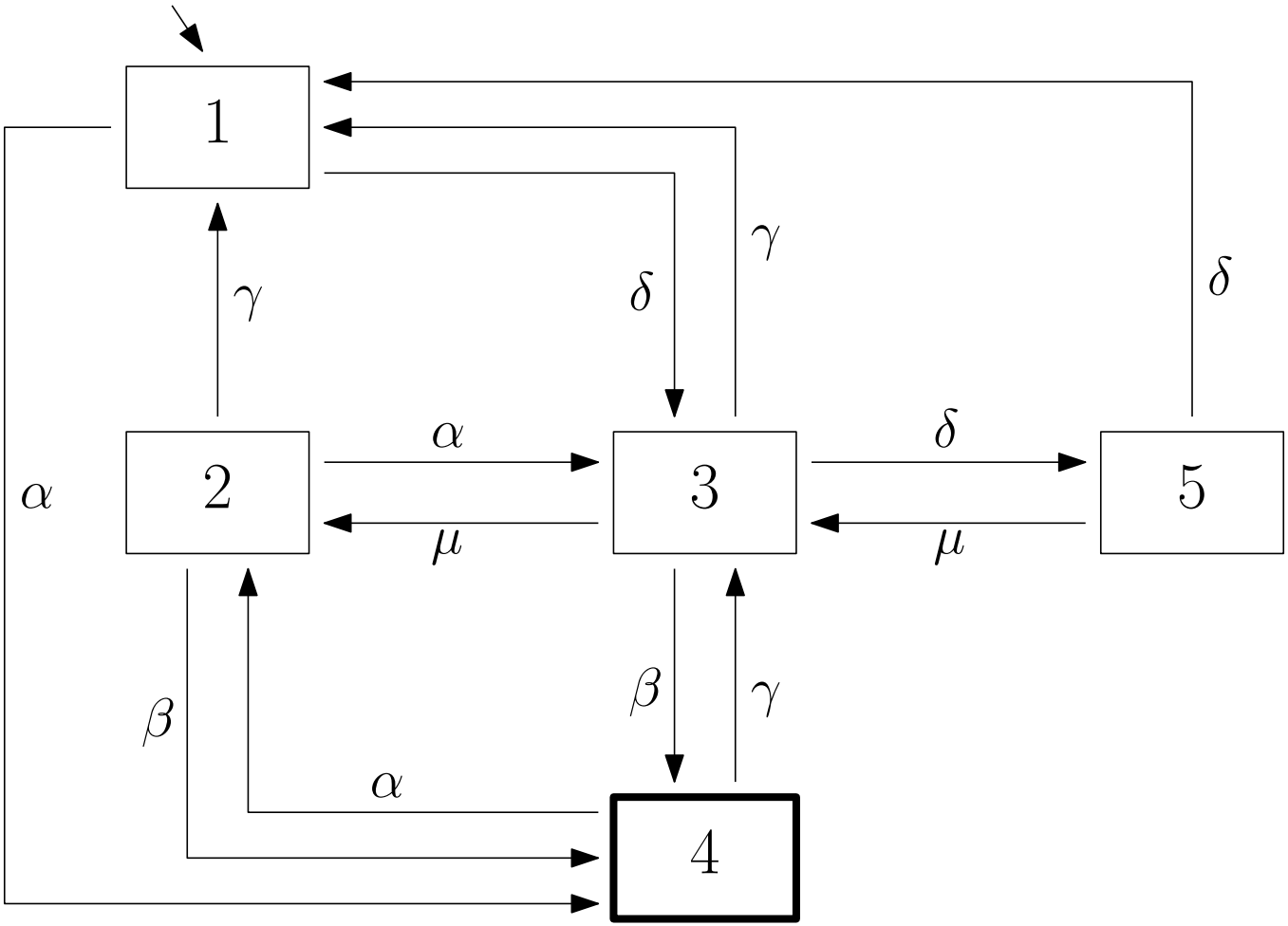
Example



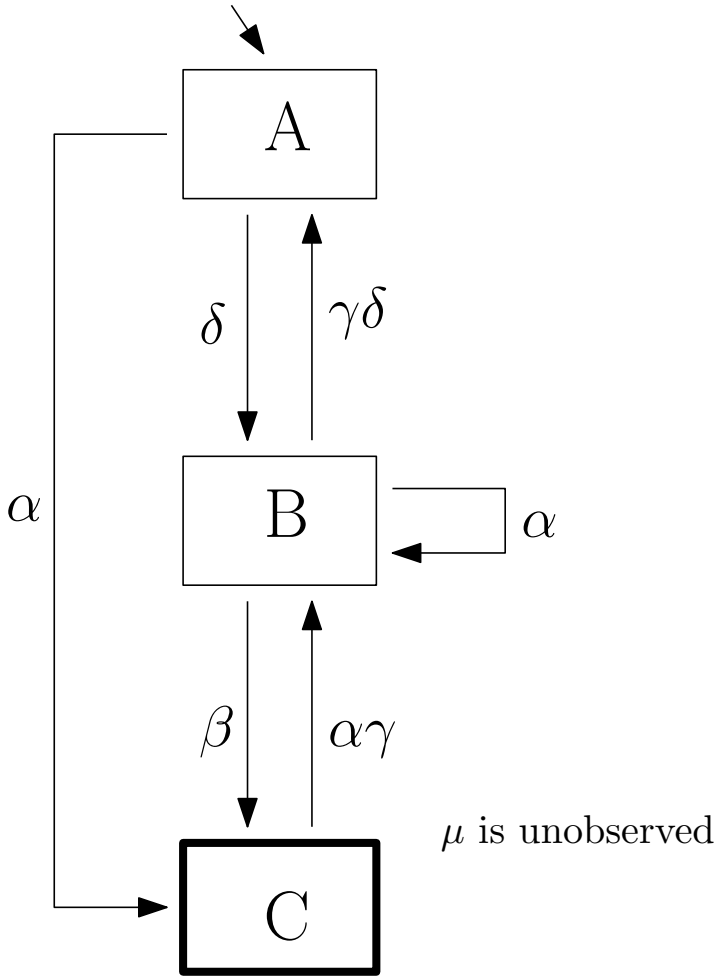
Verification by Example

- Example machine model
- Example user model
- Verification

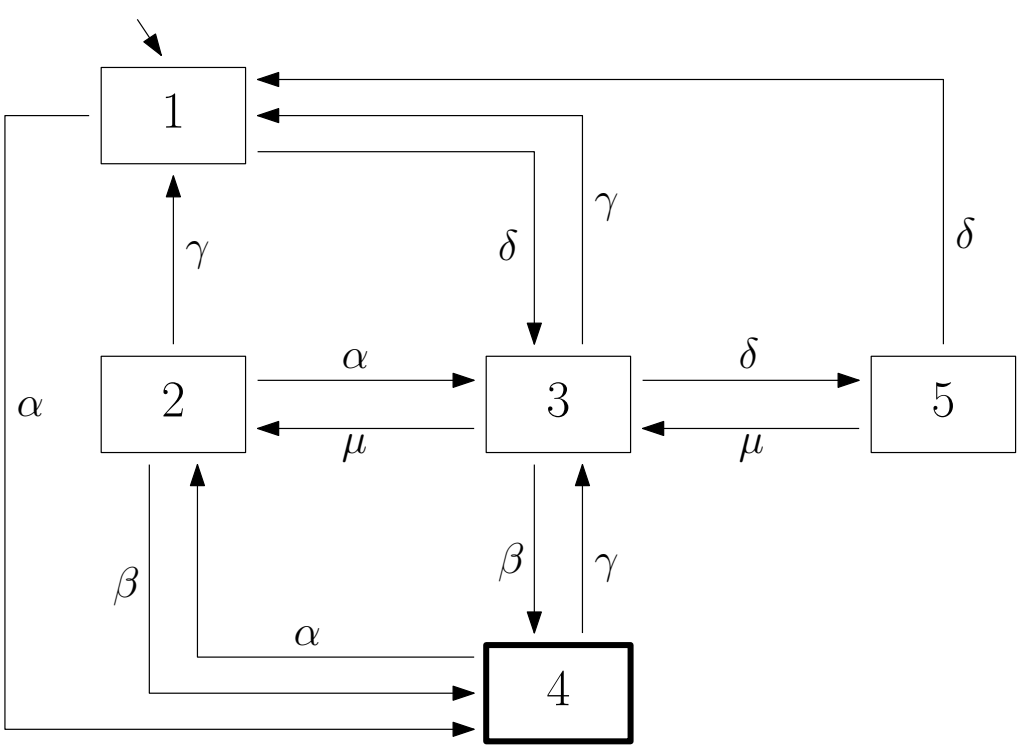
Example machine model

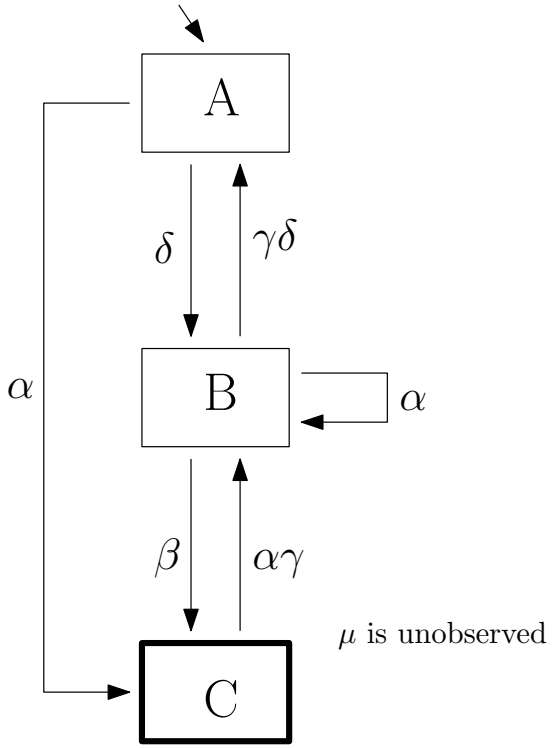


Example user model

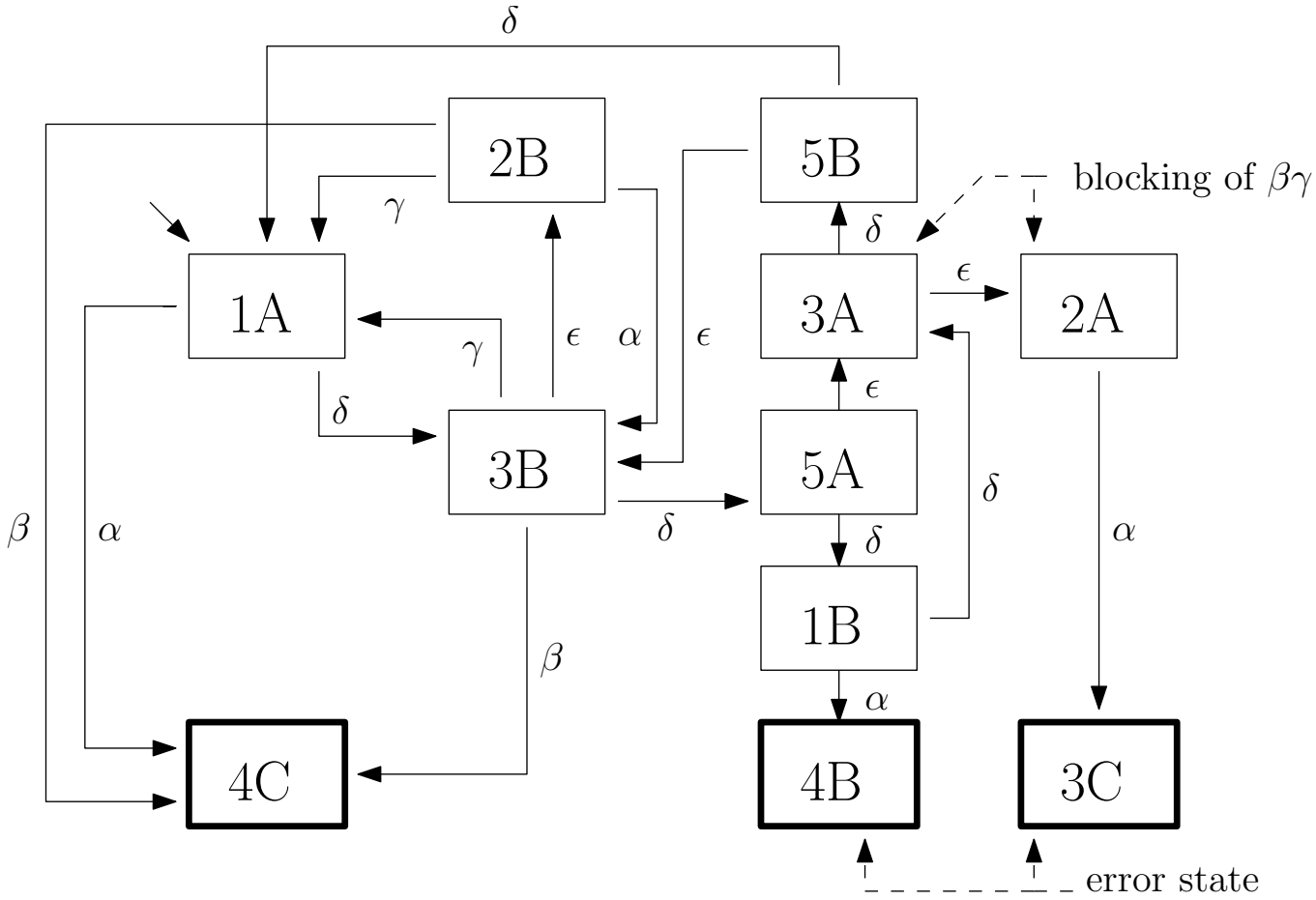


Together


1
2
3
4
5
γ
δ
γ
δ
α
α
μ
δ
μ
β
γ
α


A
B
C
δ
$\gamma\delta$
α
α
β
$\alpha\gamma$
μ is unobserved

The composite model



Construction I - Events

We describe construction of the masked synchronous product.
Σ_M - the set of events that appear in the machine model, 3 disjoint subsets:

- Σ_M^o - observed events
- Σ_M^m - masked events
- Σ_M^u - unobserved events

$\Sigma_{USR} = \Pi(\Sigma_M^o) \cup \Pi(\Sigma_M^m) \cup \Pi(\Sigma_M^u)$

- $\Pi(\Sigma_M^u) = \Sigma_M^u$
- $\Pi(\Sigma_M^u) = \epsilon$
- $\Pi(\Sigma_M^m)$ is set of events obtained after masking the events in Σ_M^m

Construction II - Transitions

In machine model: $q \xrightarrow{\alpha} q'$. Assume that user model is in state p. 3 types of events:

- observed event: in user model must exist $p'.p \xrightarrow{\alpha} p'$. In composite model $(q, p) \xrightarrow{\alpha} (q', p')$.
- masked event: in user model must exist $p'.p \xrightarrow{\Pi(\alpha)} p'$. In composite model $(q, p) \xrightarrow{\Pi(\alpha)} (q', p')$.
- unobserved event: i.e. $\Pi(\alpha) = \epsilon$, in composite model $(q, p) \xrightarrow{\epsilon} (q', p)$

Verification

What must the masked synchronous product satisfy?

- the user model does not block the machine model
- no error states with respect to the task specification

Practical aspects

- For larger systems, suitable software tools can be developed.
- The composite machine does not need to be constructed explicitly.
- Computational aspects beyond the scope of this paper.

Case Study: Automatic Flight Control Systems

- Fragment of the transition behavior of the autopilot among several vertical flight modes.
- Simple fragment, analysis can be performed manually. (suspicious?)

Data for models:

- machine model - extensive testing on flight simulator
- user-model - from the aircraft manual

Flight modes

- Hold altitude (altitude)
- Change level (target altitude)
- Vertical speed - to altitude (vertical speed, target altitude)
- Vertical speed - unconstrained (vertical speed)
- Capture altitude (altitude)

First three modes directly changed by the pilot, remaining triggered through the change of a parameter (altitude or vertical speed).

The problem

In transitions out of the capture mode:

- machine model, set altitude:
  - ahead of capture start (V/S contrained)
  - behind of capture start (V/S unconstrained)
- user model, events masked respectively into:
  - ahead of current altitude (V/S constrained)
  - behind current altitude (V/S unconstrained)

NASA's Aviation Safety Report System

On climb to 27,000 feet and leaving 26,500 feet. Memphis Center gave us a clearance to descend to 24,000 feet. The aircraft had gone to "Capture" mode when the first officer selected 24,000 feet on the GCP altitude setting. This disarmed the altitude capture and the aircraft continued to climb at approximately 300 feet-per-minute. There was no altitude warning and this "altitude bust" went unnoticed by myself and the first officer, due to the slight rate-of-climb. At 28,500, Memphis Center asked our altitude and I replied 28,500 and started an immediate descent to 24,000 feet.

- setting new altitude in capture mode
- new altitude behind the capture start altitude
- resulting in V/S unconstrained mode

Summary

- Need of formal models
- User's task - partition machine's states (legal / illegal)
- Using this technique, the correctness of the user-model can be checked
- A real problem in cockpit automation has been found!
- Only for discrete events, adaption to timed or hybrid systems an open challenge.

Discussion

Thanks for your attention.

Any questions?