

Avoiding accidents caused by human computer mismatch

assembling persuasive safety
arguments
for complex user interfaces

Luke Emmet
loe@adelard.com

Overview

- Taking a HF perspective in looking at complex systems
- Identifying HF vulnerabilities and defences
 - Namely risks arising from system degradation due to *human computer* mismatch
- Safety case needs to show risks have been reduced ALARP
 - To do this requires understanding of what the risks are
 - Safety case should explicate defences for key HF vulnerabilities
- Increases coverage of hazards
 - Completeness of hazard identification known to be an issue

General trends and evolving best practice

- Shifts in causal attribution in investigation of incidents
- Shifts in perspective of where system boundary lies
 - Systems as *Socio-Technical Systems*
- Increased recognition of centrality of humans in safety-critical systems:
 - Not just seen as an irritant - a kind of rather “faulty component”
 - Positive role in mitigation - requires participation, active control, familiarity and continual practice
 - Still central to most complex decision processes
 - Still central to most control systems

Complexity in intent

- Complex tasks - sub tasks, conditional execution
- Distributed collaborative systems
 - Multiple roles and collaboration - not just shared data but shared beliefs
 - X knows Y knows P?
 - X knows that Y knows that Z knows P?
- Real time interaction and active control loops
- Complex decision making and interpretation

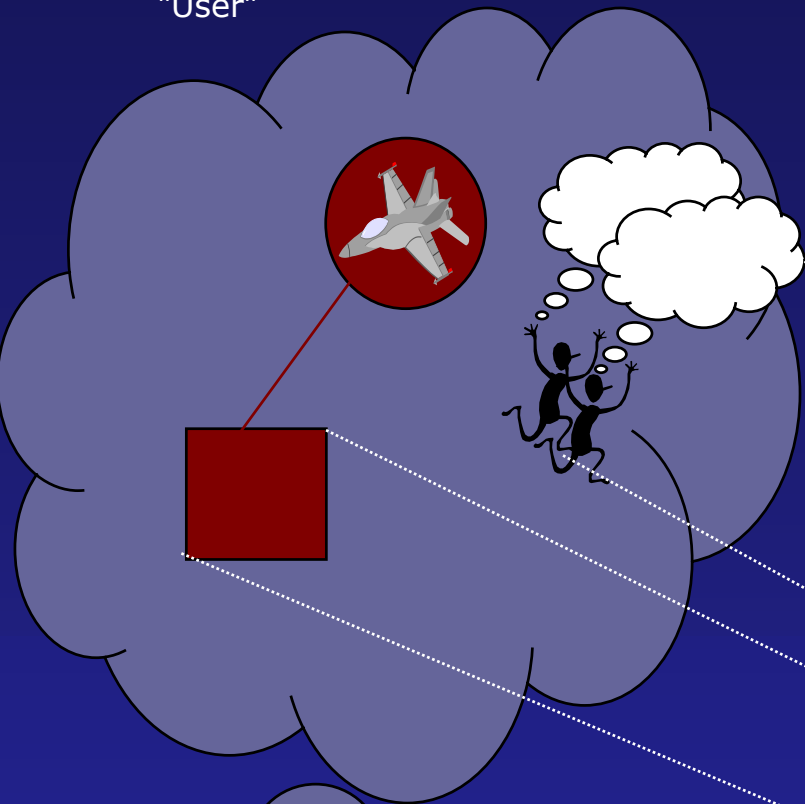
Complexity in construction

- Multiple perceptual channels
 - Visual, Aural, Tactile, Verbal
- Complex behaviours
- Complex artefacts
 - Embody core cognitive components of the system
- Bespoke software and COTS
 - Integration - user sees single system
 - COTS - someone else's user model

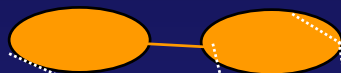
The nub of the issue

- General call for transparency and consistency
 - User model, state & behaviour \Leftrightarrow System, state & behaviour \Leftrightarrow The affected world
- But for complex systems the user cannot directly perceive the system and its state, and relies on:
 - Complex representations and associated behaviours
 - Interpreting these to update his/her mental model
 - Forming (correct?) beliefs about the system and the world
 - Various expectations: task enactment; normative behaviour & doctrine; training

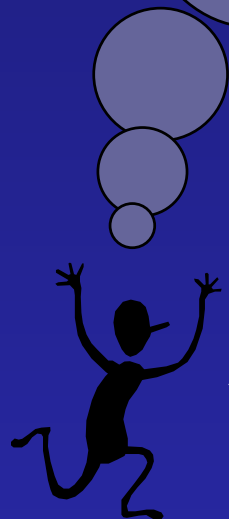
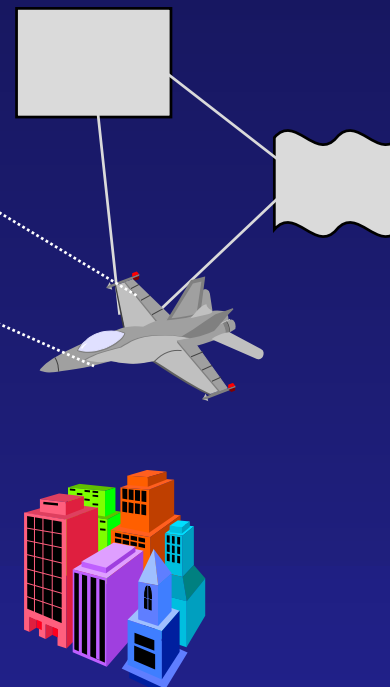
"User"



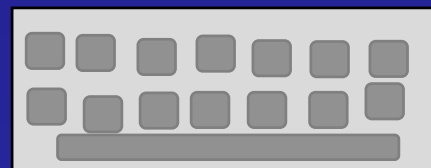
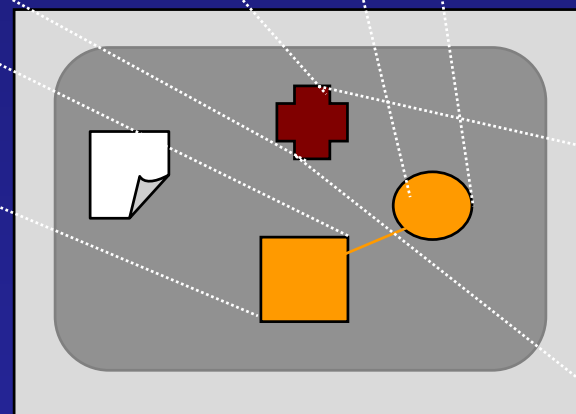
"System"



"World"



Visual, Auditory,
Psychomotor,...



User interface



Drivers for degradation - key vulnerabilities

- Wrong task model
- Poor UI design
 - Both widgets and behaviour
- Errors in execution
 - finger trouble etc.
- Inadequate feedback
- System autonomy and modal behaviour
- Cultural mis-projections:
 - e.g. use of colour and terminology
- COTS boundaries
- Unexpected user model
 - Stress - reversion to simple user model
 - Expectations from previous systems
 - Unusual scenarios

Assembling persuasive HF safety arguments

- Argue that design activities conducted from basis of a rich system model that acknowledges scope for de-synchronisation
- Argue sufficient safety and HF integration
 - Need to show understanding of how potential mismatches can impact the safety of the designed system
 - Need to show defences to key HF vulnerabilities
- Demonstrate a consistent and coherent approach to system as a whole
 - Selection and integration of COTS

Clear safety role for classical HF tasks

- HF Integration and user centred design
- Sufficient task characterisation analysis and synthesis
 - Needs to address actual, not just idealised model
- HCI risk identification
- HCI evaluation
 - Errors in behaviour; errors in execution; adequate performance, not just based on user satisfaction
 - Desk based analysis

Provides evidence for safety case

Conclusions

- Safety cases need to be based on richer models of socio-technical systems
 - Understand scope for de-synchronisation
- Safety claims about user interfaces not just about “knobs and dials” and user satisfaction
 - User model, task expectations, collaborative beliefs
- Integrated design processes needed to move beyond demarcated responsibilities:
 - HCI, System design, Safety management

Thank you

Any questions?