City University London

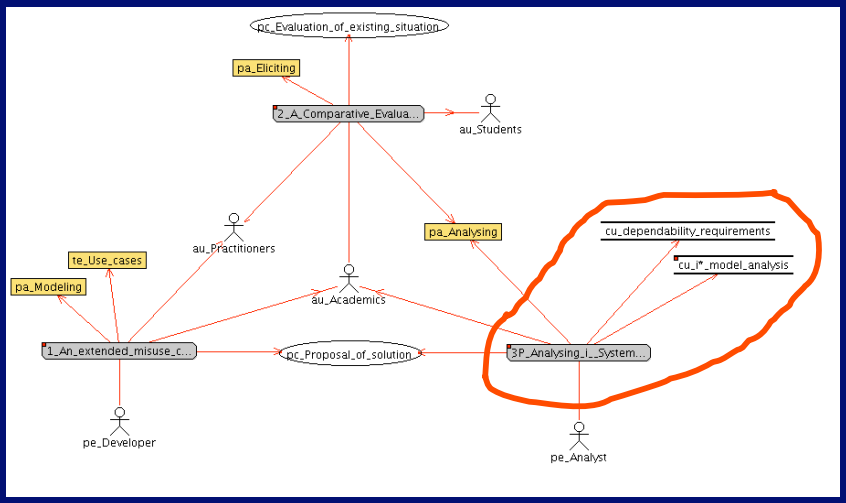
Analyzing i* System Models for Dependability Properties: The Uberlingen Accident

Neil Maiden[1], Namit Kandar[1] and David Bush[2]
City University[1], Ascolto Ltd UK[2]

Centre for HCI Design

City University London

First Slide



City University London

Centre for HCI Design

Analyzing Dependability Properties

Pressing need in requirements

- Determine properties such as reliability and safety of socio-technical systems
- Methods such as HAZOPS not always suitable
- Can requirements models such as *i** help?

Exploratory retrospective analysis

- Model socio-technical systems during Uberlingen air accident in 2002 using *i**
- Analyze *i** models with derived treatments
- Explore whether classes of problems that occurred might have been predicted
- Refine and re-apply treatments to other case studies

City University London

Centre for HCI Design

Uberlingen Accident

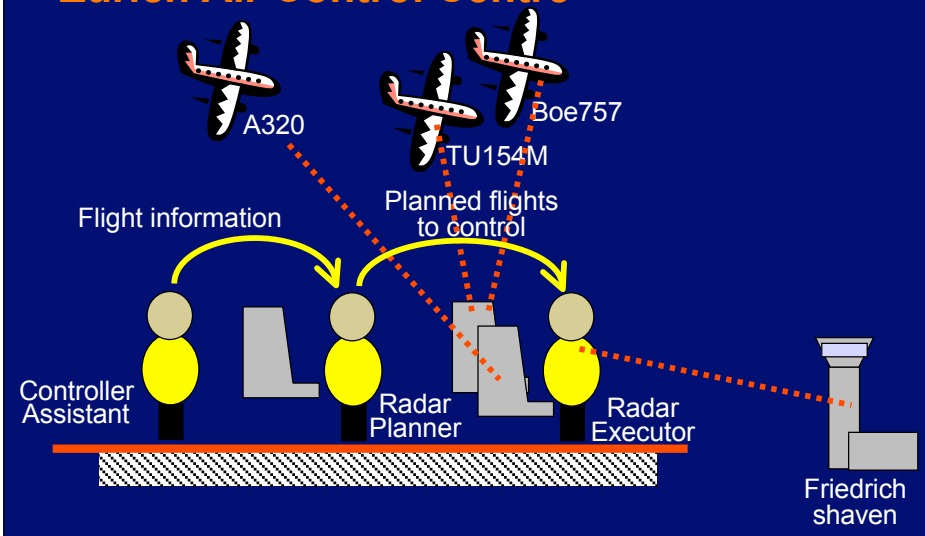
Evening 1st July 2002, in Swiss-controlled air space

Two planes collided in mid-air, killing 71

City University London

Centre for HCI Design

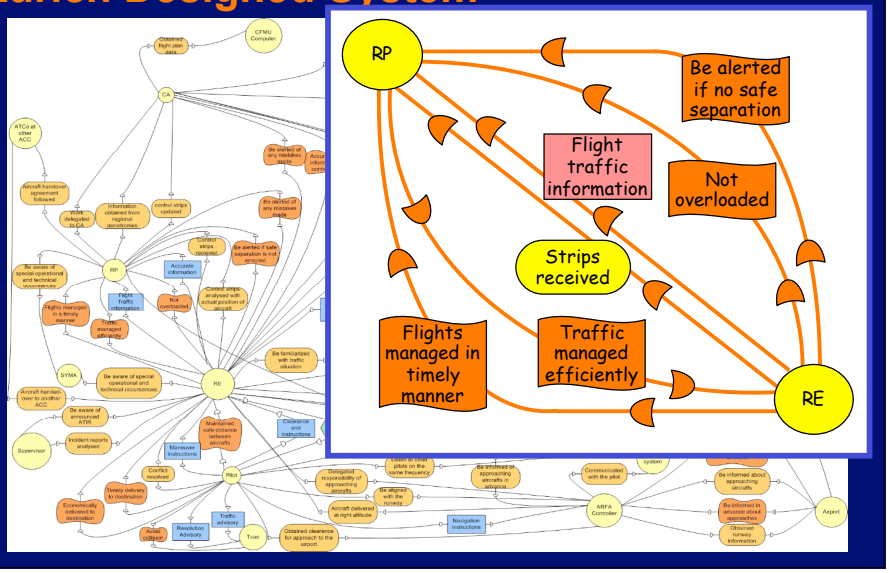
Zurich Air Control Centre



City University London

Centre for HCI Design

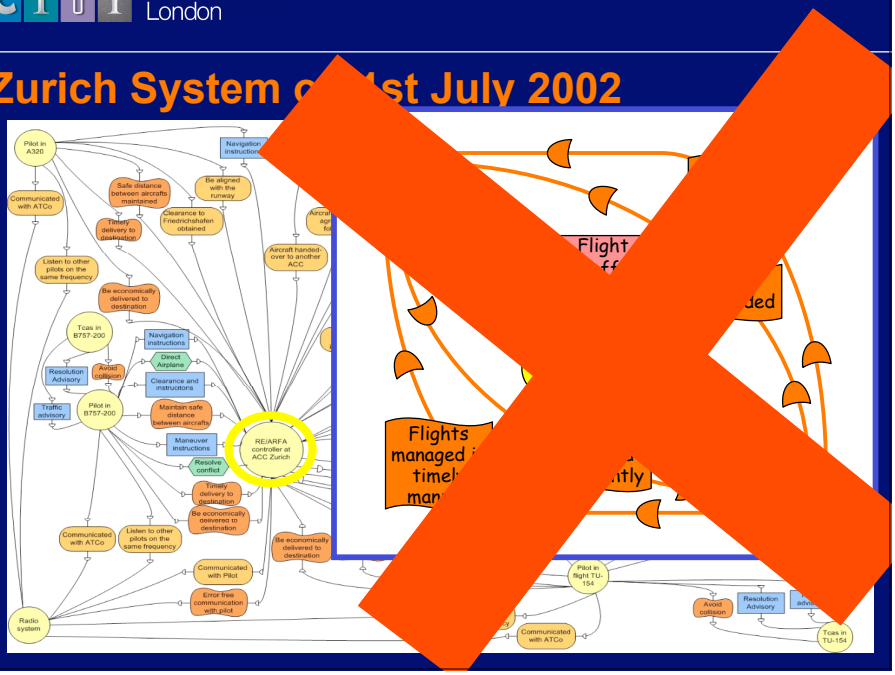
Zurich Designed System



City University London

Centre for HCI Design

Zurich System c st July 2002



City University London

Centre for HCI Design

Analytic Treatments

1. Increased actor dependencies
   - If actor fulfils 2 or more roles, do additional dependencies risk overloading dependee actor
   - RE was dependee in 17 rather than 10 dependencies
   - Indicative of increased actor workload
2. Unachieved goals and soft goals
   - RE actor cannot achieve critical soft goal *not overloaded* if RP not present
   - But need to extend expressiveness of *i** models with KAOS patterns [Darimont & van Lamsweerde 1996]
   - Infer FAIL TO ACHIEVE if dependee not present
   - Not all missing dependencies are detrimental

Future Work

Develop formal heuristics

- Analyze formally-expressed dependability properties of socio-technical systems expressed as *i** SD and SR models
- Derive from diverse sources including published requirements and safety-critical case studies
- Extend *i** expressiveness with KAOS goal patterns
- Re-apply to other case studies

Extensions to REDEPEND

- Explore use of actor agents, roles and positions in *i**
- Implement formal heuristics in graphical tool to analyse system models to inform early requirements analysis

City University London
Centre for HCI Design

Conclusions

Quality features addressed

- Dependability properties such as reliability and safety

Novelty and contribution

- Integrating important treatments in RE representations

Contribution to research and practice

- Exploration of scaleability and applicability of RE research outcomes to real problems

Main problems

- Position paper applied to one case study

Scaleability

- Do not know yet!