DIRC

EPSRC

Engineering and Physical Sciences
Research Council

UNIVERSITY OF
NEWCASTLE

DIRC

www.dirc.org.uk

THE UNIVERSITY OF EDINBURGH

THE UNIVERSITY of York

# Dependability: an Interdisciplinary Research Collaboration

LANCASTER
UNIVERSITY

CITY
City University
London

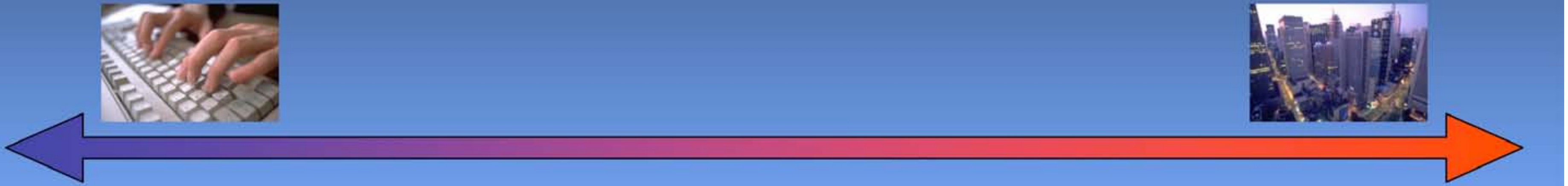
# HUMAN-MACHINE INTERACTION in CRITICAL SYSTEMS

Denis Besnard
School of Computing Science
University of Newcastle upon Tyne
denis.besnard@ncl.ac.uk

# Outline

1. The spectrum of human error
2. Two cognitive biases
3. Mode confusion and biases
    - The Kegworth aircrash
    - The Royal Majesty grounding
    - The Mont Sainte Odile aircrash
4. Lessons and beyond…
5. Anticipative systems needed
6. Where are we?
7. What are the next steps
8. It can be done
9. Conclusion

# 1. The spectrum of human error



**Cognitive dimension**

- Erroneous knowledge
- Cognitive limitations
- Heuristics & biases

*Rasmussen*

*Reason*

**Social cog. dimension**

- False beliefs
- Stereotypes
- Illusory correlations
- Salience effect
- Social categorization

*Tversky & Kahneman*

**Social dimension**

- Organisation
- Power
- Leadership
- Team working

*Lewin, Lipitt & White*

*Milgram*

*Festinger*

# 2. Two cognitive biases

**Confirmation bias**

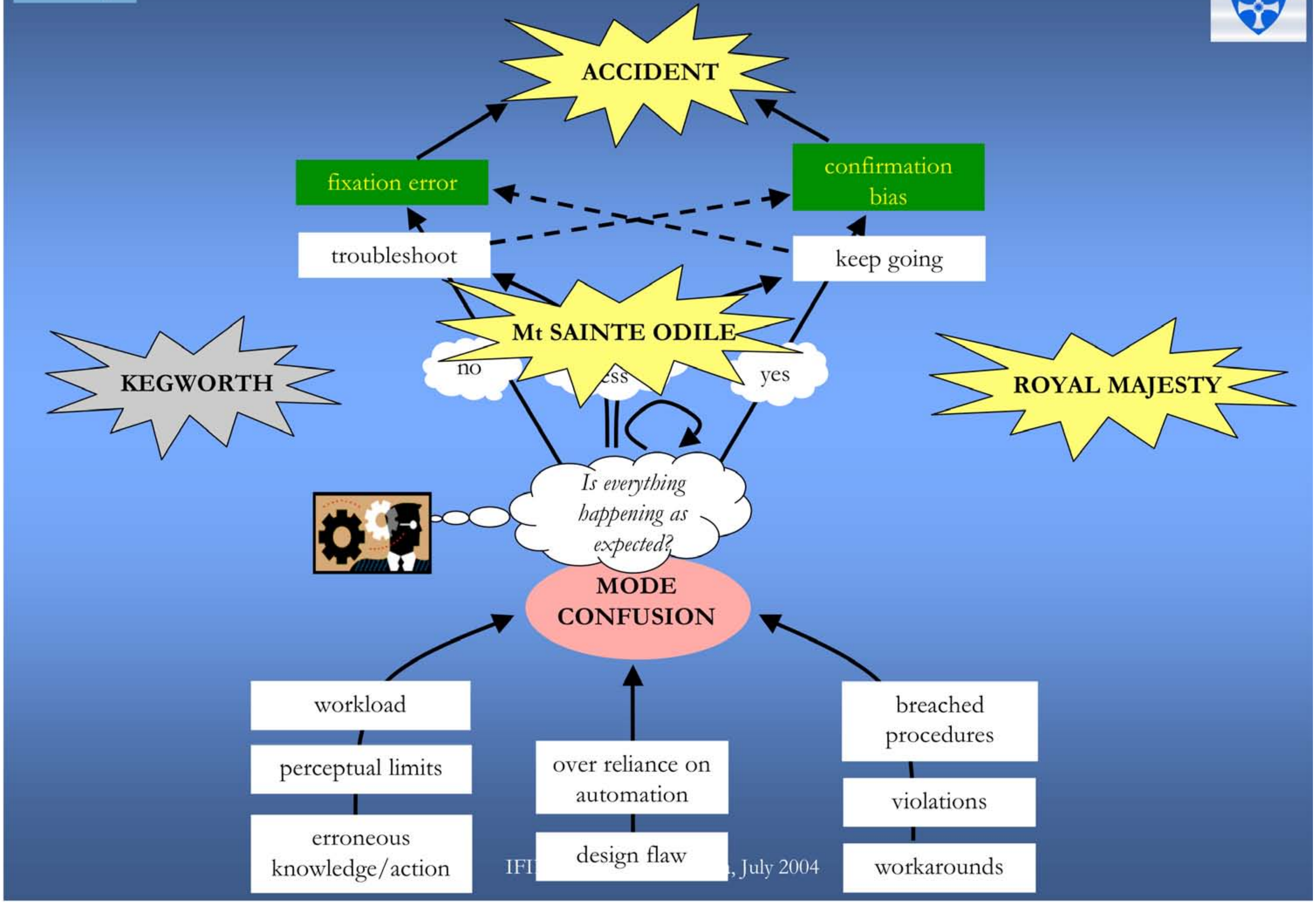
Testing a hypothesis by cases that attempt to confirm it rather than cases that could reject it.

**Fixation error**

For a given problem, defining a too narrow set of causes and searching within this set.

- These biases are caused by cognitive resources saving measures (e.g. heuristics)
- Mode error + cognitive bias = Potential accident

# 3. Mode confusion and biases

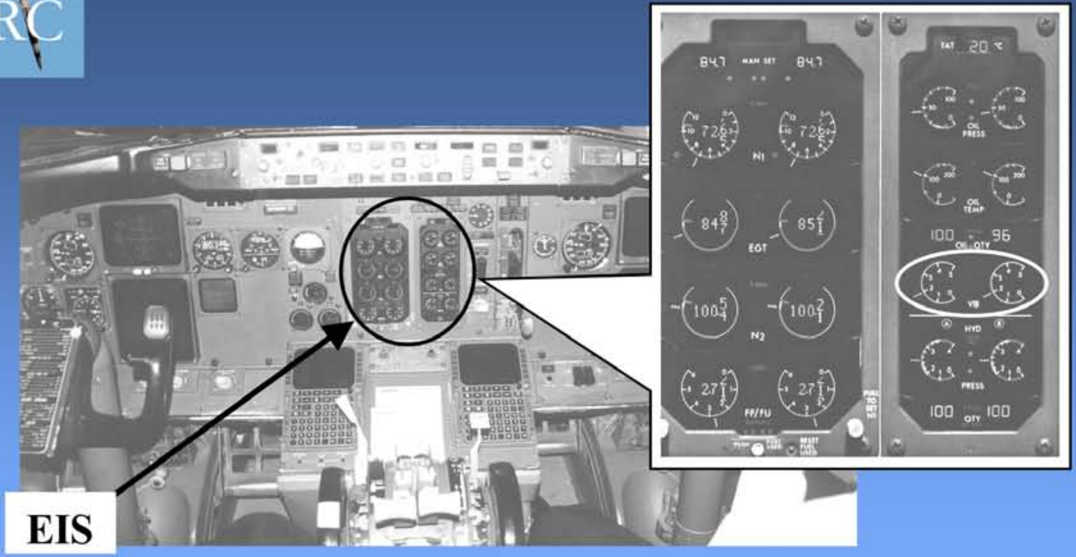


# Outline

1. The spectrum of human error
2. Two cognitive biases
3. Mode confusion and biases
   - The Kegworth aircrash
   - The Royal Majesty grounding
   - The Mont Sainte Odile aircrash
4. Lessons and beyond…
5. Anticipative systems needed
6. Where are we?
7. What are the next steps
8. It can be done
9. Conclusion

# The Kegworth aircrash, 1989

(c) / Source: AAIB Aircraft Accident R



- Vibrations on left engine
- Crew shut down other engine but symptoms stopped
- Co-occurrence leading to biased mental model
- Recovery attempted too late.
- Crash at 0.5 mile from runway.

## Error recovery can be made difficult because of a confirmation bias

- OK, not really about mode confusion…
- Initial slip (error) not an issue
- Not recovering IS the issue
- The crew thought they had solved the problem

WHY?

- Because an event (ceasing of vibrations) occurred as expected
- Humans are overconfident about things happening as expected

# The Royal Majesty grounding, Nantucket, 1995

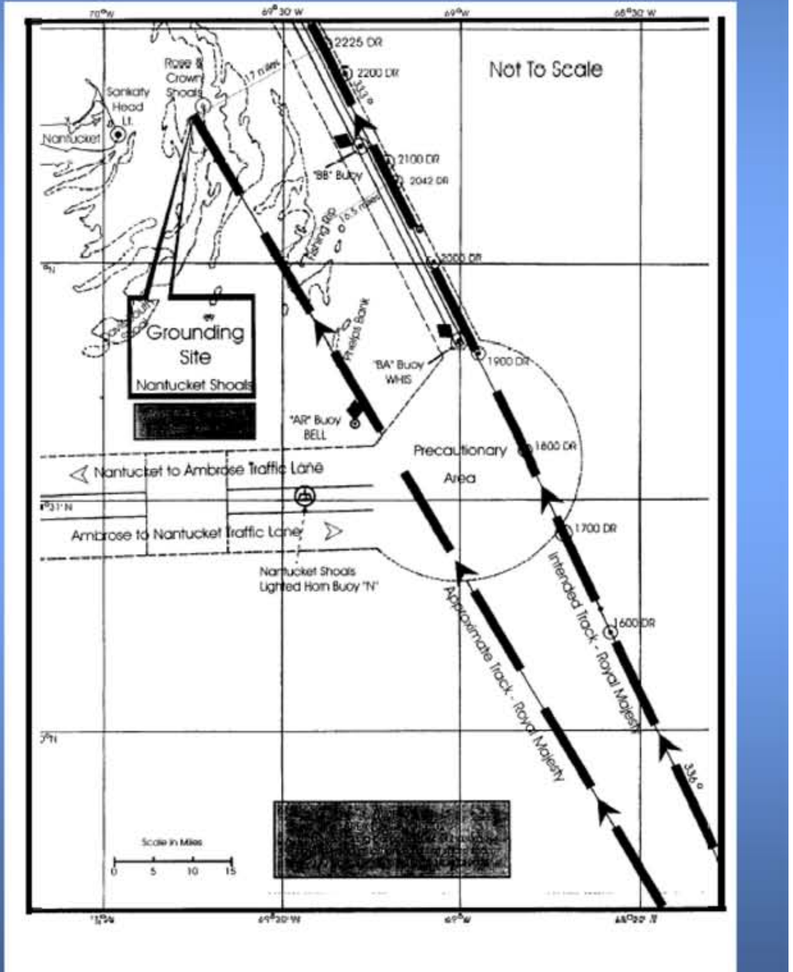


Figure 5-Intended track and approximately actual track.

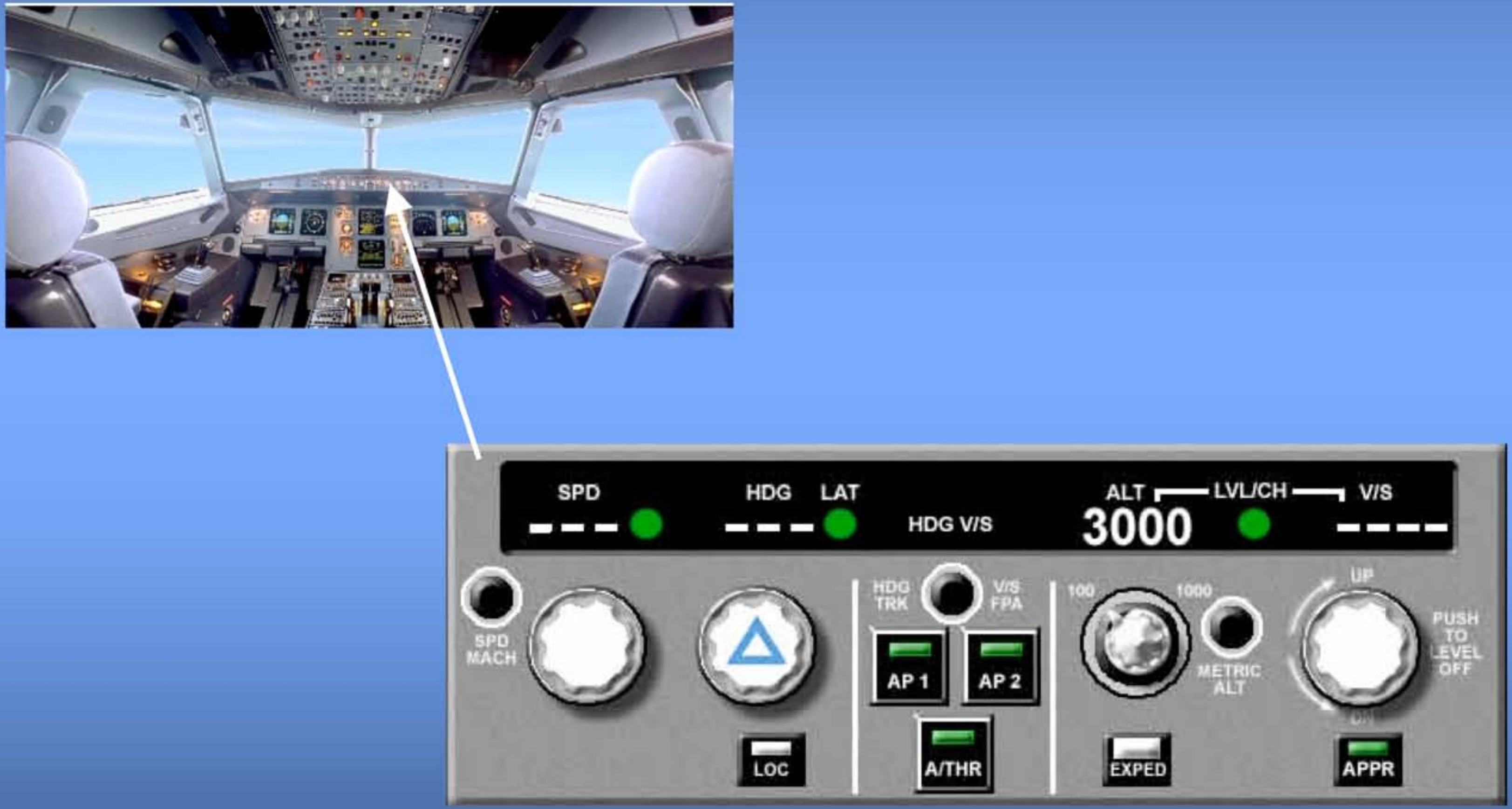
- GPS cable disconnected.
- GPS switched silently to DR mode
- Mode change not noticed by crew
- From there on, wrong position awareness

# Mode confusion can be hard to detect

- Crew did not know their precise position
- Further consistent cues overestimated (AR buoy taken as BA)
- Further inconsistent cues disregarded (lights, blue & white water)
- Recovery is made more and more difficult as further cues fit the mental model
- These aspects not thoroughly investigated in the accident report

# The Mont Sainte Odile air crash, 1992

- Aircraft approaching Strasbourg, France.
- Crew intending to fly around the airport and land from far end of runway
- ATC suggests direct landing
- Crew has to reprogram the descent: big increase in workload
- FPA/VS confusion
- 3.3 degrees turned into 3300 feet/min: too fast
- Landing gear alarm sounded but crew couldn’t interpret
- Crash into Mont Sainte Odile. Only 6 people survived



A320 Flight Control Unit

## Mode confusion can be hard to recover from

- Crew made a slip in programming the descent
- They did not detect the erroneous mode
- Flawed vertical position awareness due to too fast sink rate
- Alarms were not interpreted meaningfully
- Strong time constraints

# Outline

1. The spectrum of human error

2. Two cognitive biases

3. Mode confusion and biases

  - The Kegworth aircrash

  - The Royal Majesty grounding

  - The Mont Sainte Odile aircrash

4. Lessons and beyond…

5. Anticipative systems needed

6. Where are we?

7. What are the next steps

8. It can be done

9. Conclusion

# 4. Lessons and beyond…

- Humans in complex systems have an important supervisory role
- They have to be in the control loop for high-level decisions and exceptions
- Modern systems have more and more autonomy (FMS, GPS-driven autopilots, ILS)

- Humans make errors
- Reality can be twisted to fit the mental model
- Modern automation in not always transparent nor predictable (see Chris Lawrence, bluecoat)
- Problem of modes design and awareness in computer-based interfaces

Anticipative systems needed

Where are we?

What are the next steps?

# 5. Anticipative systems needed

- *Flight Safety Foundation 1999 report:* 287 fatal approach and landing accidents between 1980-1996. The two main causes were lack of position awareness + omission-commission of action.
- *1996 FAA report* on modern flightdeck interfaces. Two many modes, not enough transparency nor predictability.

- Humans exhibit best performance when they are "ahead" of the system (Woods, Amalberti, …)
- Systems need to know something about the operator to detect departures from optimal interaction.
- Anticipative systems based on plan recognition cannot help for unexpected events but many accidents happen within nominal conditions.
- CATS (Callantine) implemented on experimental B757 at NASA Ames

# 6. Where are we?

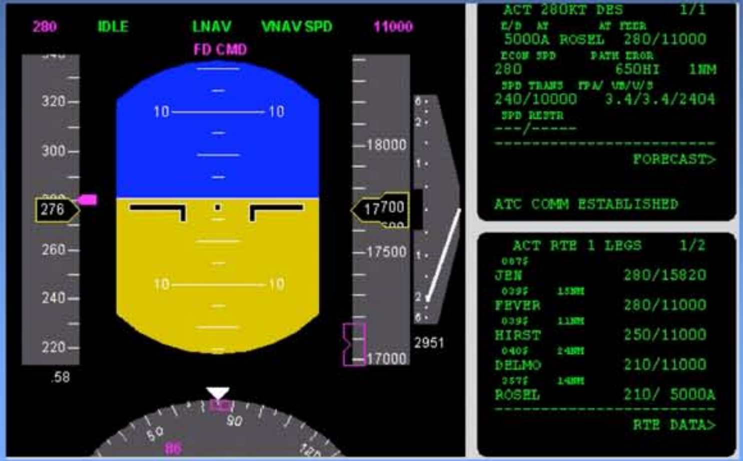
**Prevot & Palmer, 2000**

Vertical flight path is one of the most problematic areas in glass cockpits.

- 12 experimental crews have to fly 7 descents on a B757 simulator.

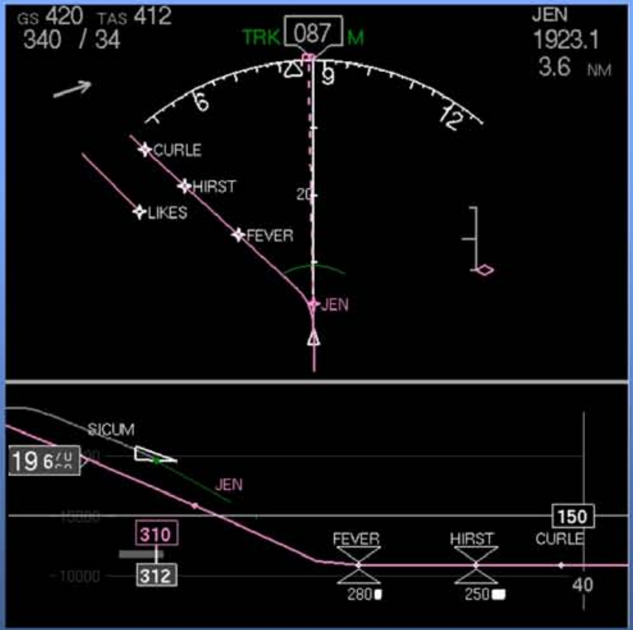
- Experimental crews feel more ahead of the airplane with Vertical Situation Display than with conventional interface.

- VSD helped crews understand how the FMS manages the flight path.



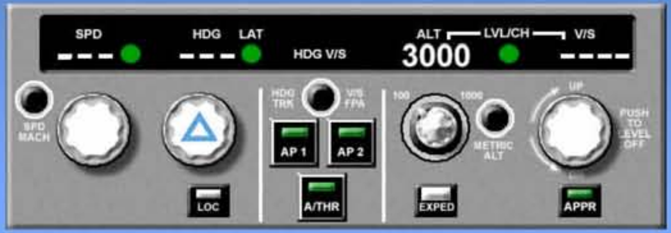
```
ACT 280KT DES        1/1
 E/D AT      AT FEER
 5000A ROSEL  280/11000
 ECON SPD    PATH EROR
280            650HI   1NM
 SPD TRANS  FPA/ VB/V/S
240/10000   3.4/3.4/2404
 SPD RESTR
---/-----
------------------------
             FORECAST>

ATC COMM ESTABLISHED
```

```
  ACT RTE 1 LEGS     1/2
 087°
JEN                280/15820
 039°    15NM
FEVER              280/11000
 039°    11NM
HIRST              250/11000
 040°    24NM
DELMO              210/11000
 357°    14NM
ROSEL              210/ 5000A
------------------------
              RTE DATA>
```



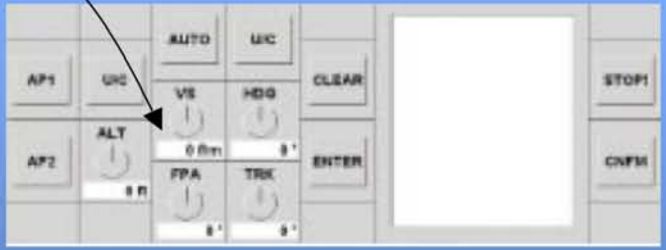
# Hourizi & Johnson, 2001

Redesigned and tested a modeless A320 Flight Control Unit



- Mutually exclusive functions are now grouped in columns

-The programming goes from left to right



- Experimental task: FCU programming using Mont Sainte Odile condensed transcript

- 40% of subjects made the same mode error as the actual Mont Sainte Odile pilot with conventional interface

- 0% error rate with new interface

## Dehais *et al.*, 2003

Tested a PC-driven interface that prevents fixation errors (GHOST)

- Results show that blanking, blinking and fading catch pilots' attention

- Text-based messages are then taken into account

# Leveson & Palmer, 1997

Accidents may result from any of the models (in Fig 2) being incorrect or becoming inconsistent with the true state of the controlled process, the automated controller, or the supervisory interface (the human-computer interface).

The process model is based on:

1. Current process state inferred from measured variables,

2. Past measured and inferred process states and variables,

3. Past outputs to actuators, and

4. Prediction of future states of the controlled process.

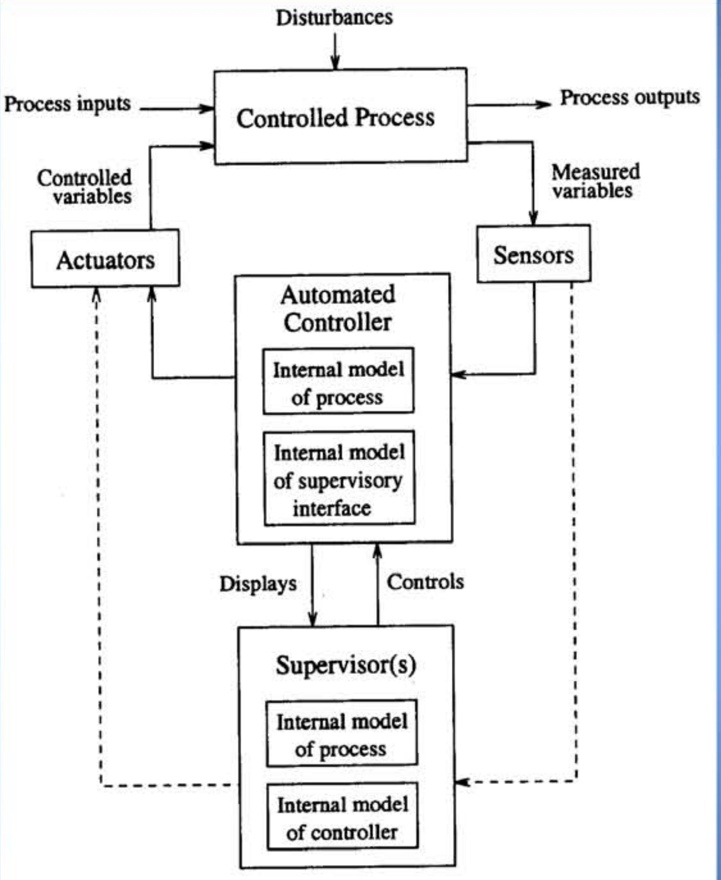
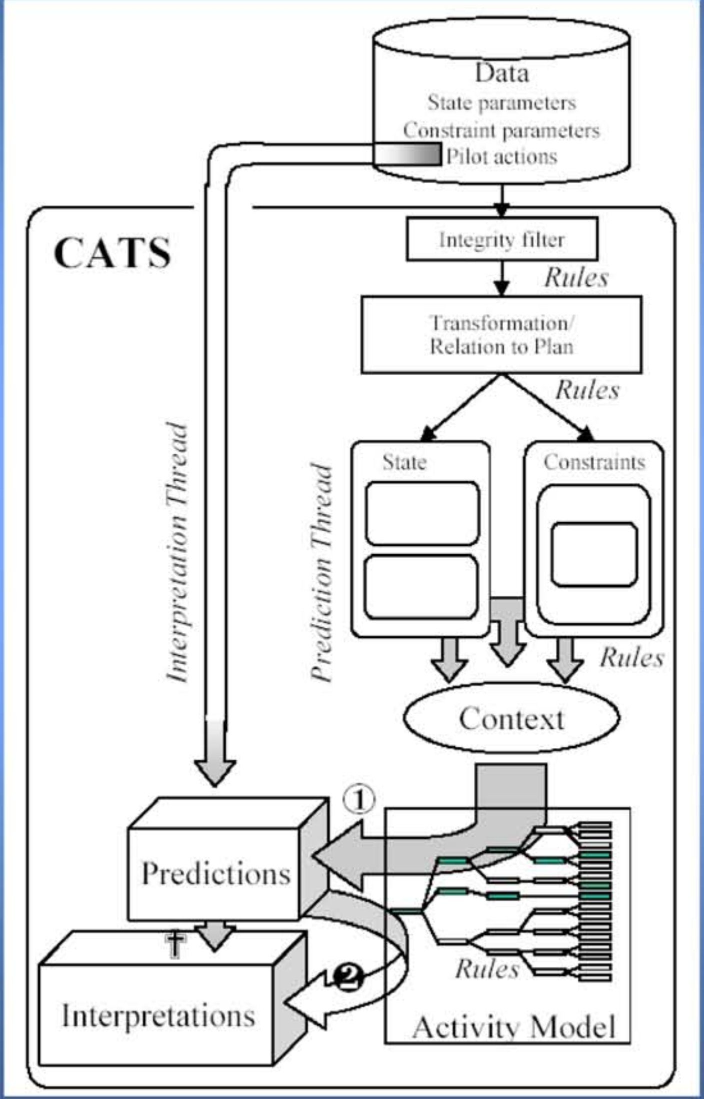


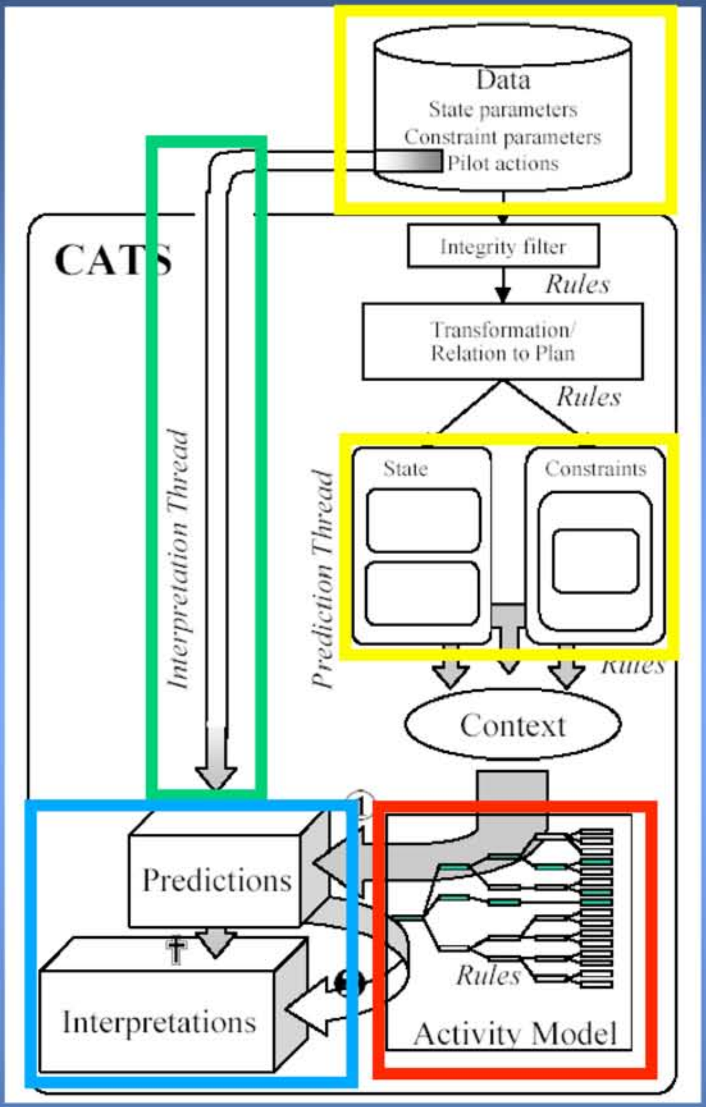
Figure 2: Modified Model to Account for Operator Error and Mode Confusion.

# Callantine, 2000

Designed and implemented CATS on an experimental B757 at NASA Ames

- Compares pilot's actions to nominal plans according to operational context
- Prompts pilot if actions need completion in given timeframe





Data gathered during flight

Interprets pilot's actions

Used to derive operational context

Various ways to perform task

Mismatches?

Flags error and displays a few lines of text to cue pilot.

# Outline

1. The spectrum of human error
2. Two cognitive biases
3. Mode confusion and biases
   - The Kegworth aircrash
   - The Royal Majesty grounding
   - The Mont Sainte Odile aircrash
4. Lessons and beyond…
5. Anticipative systems needed
6. Where are we?
7. What are the next steps?
8. It can be done
9. Conclusion

# 7. What are the next steps?

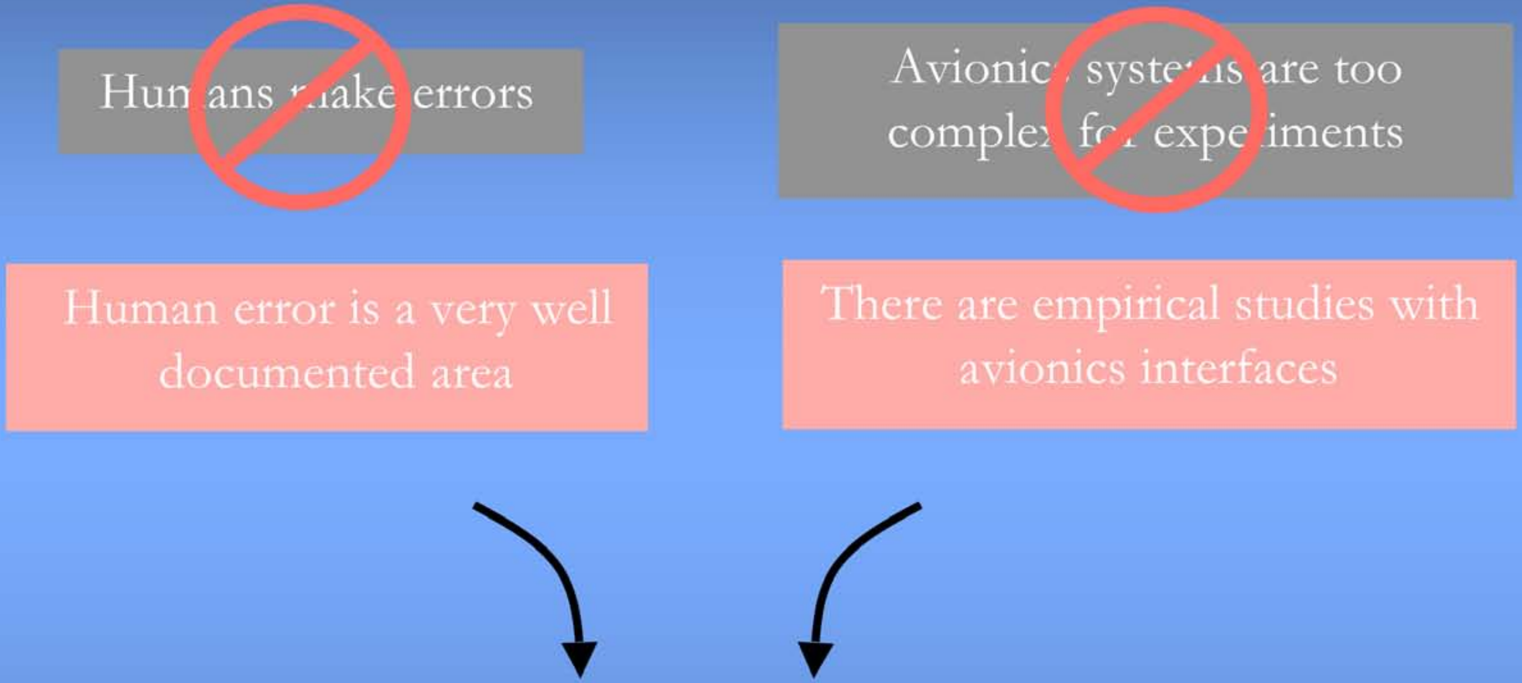
**Short term**

- Replicate accidents (cross-domain?).
- Identify critical variables to loss of (mode) awareness. What is needed for it to trigger (e.g. confirmation of expectancies)?
- Play with variables to see conditions under which detection/recovery is facilitated.

**Long term**

- Give the system a model of itself and expectancies (Callantine)
- Importance of detection of inconsistencies between operator's intentions and actual/foreseen events
- The system must "understand" the operator's decisions (remember Kegworth!)
- Allow the system to suggest options to the operator

# 8. It can be done!



~~Humans make errors~~

~~Avionics systems are too complex for experiments~~

Human error is a very well documented area

There are empirical studies with avionics interfaces

More industrial collaboration is what we now need

Stop publishing. Do some real work.

# 9. Conclusion

- Mode confusion happens because of modes number/complexity/interaction (e.g. indirect mode changes)
- Mode-based accidents happen because of mode confusion can go undetected
- Anticipative systems are needed to keep operators "ahead of the system"
- Experiments are needed to define key design parameters and philosophies

- Accident rate in industrialised countries is below 1 per million departures
- Airplanes are technically safer than ever
- Accidents in the future (e.g. CFITs) will mainly be caused by HMI