“Spoilers! Reverse Green! Decel!” or What’s it doing now?

Thoughts on Automation in Aviation and its Human Interface

Bernd Sieker

Universität Bielefeld, CITEC

December 2010

“Spoilers, Reverse Green, Decel”

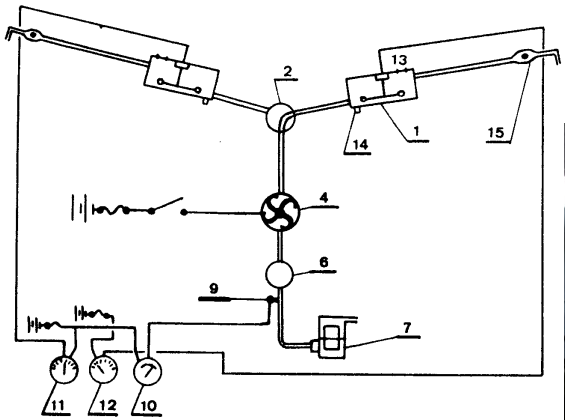
- What’s it Doing Now?
- Video: A good approach in an Airbus A320
- Video: A Bad Flyby

Complexity: Fuel Systems

Compare:

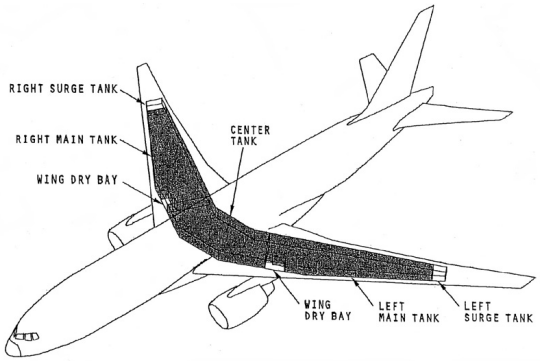
- Socata Rallye 100ST, small 2–3 seat airplane

one engine, two tanks

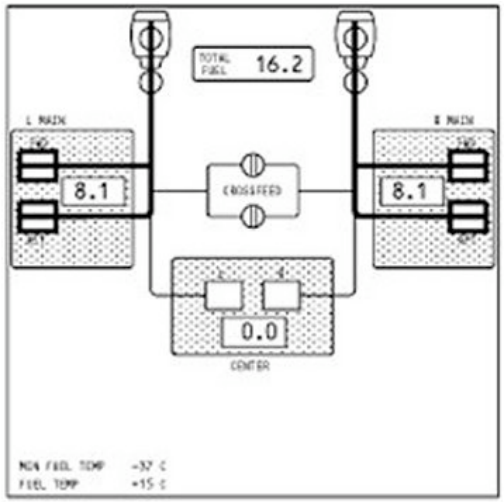


Complexity: Fuel Systems -2-

- Boeing B777, wide-body airliner, long-haul workhorse
  - Two engines, three tanks

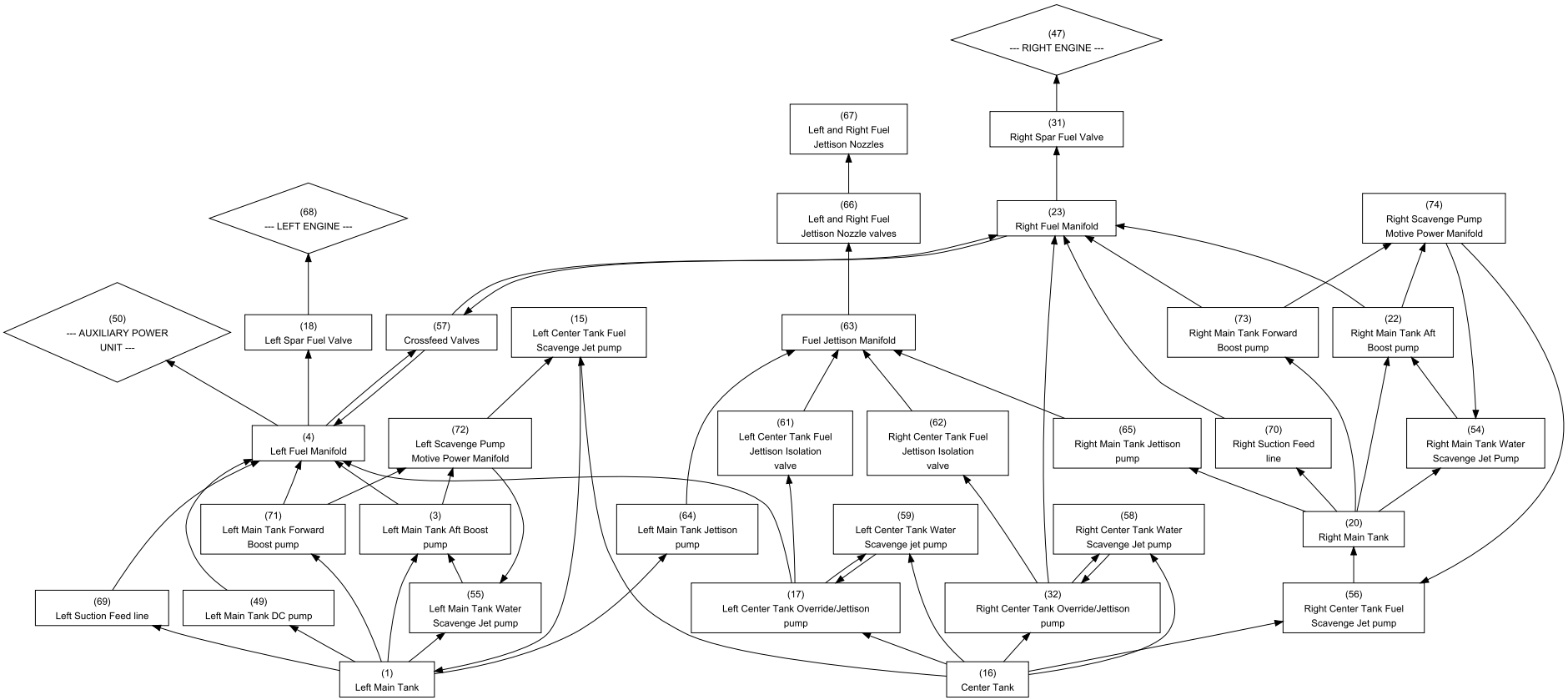


  - How much more complicated can it be? Not that much, right?



Complexity: Fuel Systems -3-

Actually: Quite a lot ...



(That's just tanks, pumps, valves in the airframe. Excluding engines.)

What to Show? What to Withhold?

- Avoid overload
- Show all information needed to make decision
- highly non-trivial
- Too many lights: “Christmas Tree”
- Too many sounds: “Cacophony”
- Too little information: suboptimal decisions
- A huge part of status display system software: prioritization

British Airways Flight 038

- Boeing 777
- Insufficient engine thrust during final approach
- Exceptional Crew performance
- Barely cleared the perimeter fence
- Landed in the grass, skidded up to runway threshold
- Extensive damage, ruptured fuel tanks, pierced wings, etc.
- No fire
- No fatalities

Video: ATC

BA-038 — Cockpit indications

- Possibly fuel pipe icing
- Autothrottle demanded thrust increase
- FADEC commanded fuel metering valve opening
- fuel flow increase was less than demanded
- No cockpit indications of discrepancy
- $\Rightarrow$ problematic situation was detected late
- Balance of what to show/withhold?

Spanair — Crash in Madrid

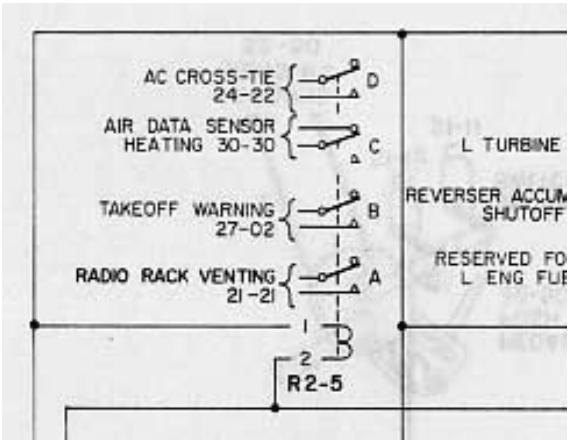
(Photo: 54north[1])

- MD80 crew notices excessive Ram-Air Temperature (RAT) indication
- Return to Gate (retracting Flaps)
- Technician pulls RAT-probe heating circuit breaker
- Dispatch according to Minimum Equipment List (MEL)
- Aircraft takes off without flaps
- Climbs to 40ft, descends, crashes

[1] http://commons.wikimedia.org/wiki/User:54north

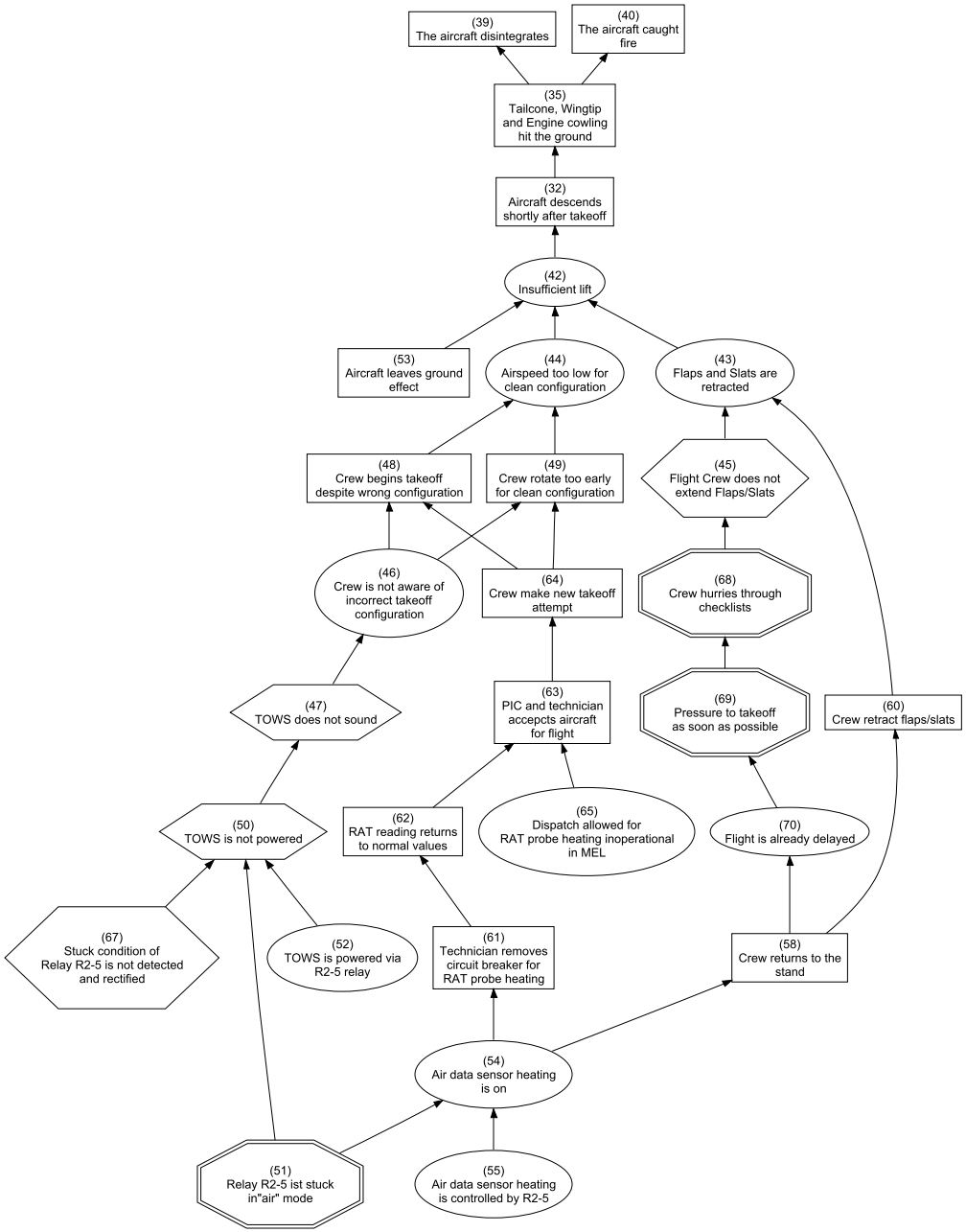
Spanair Accident — What happened?

- Relay R2-5:

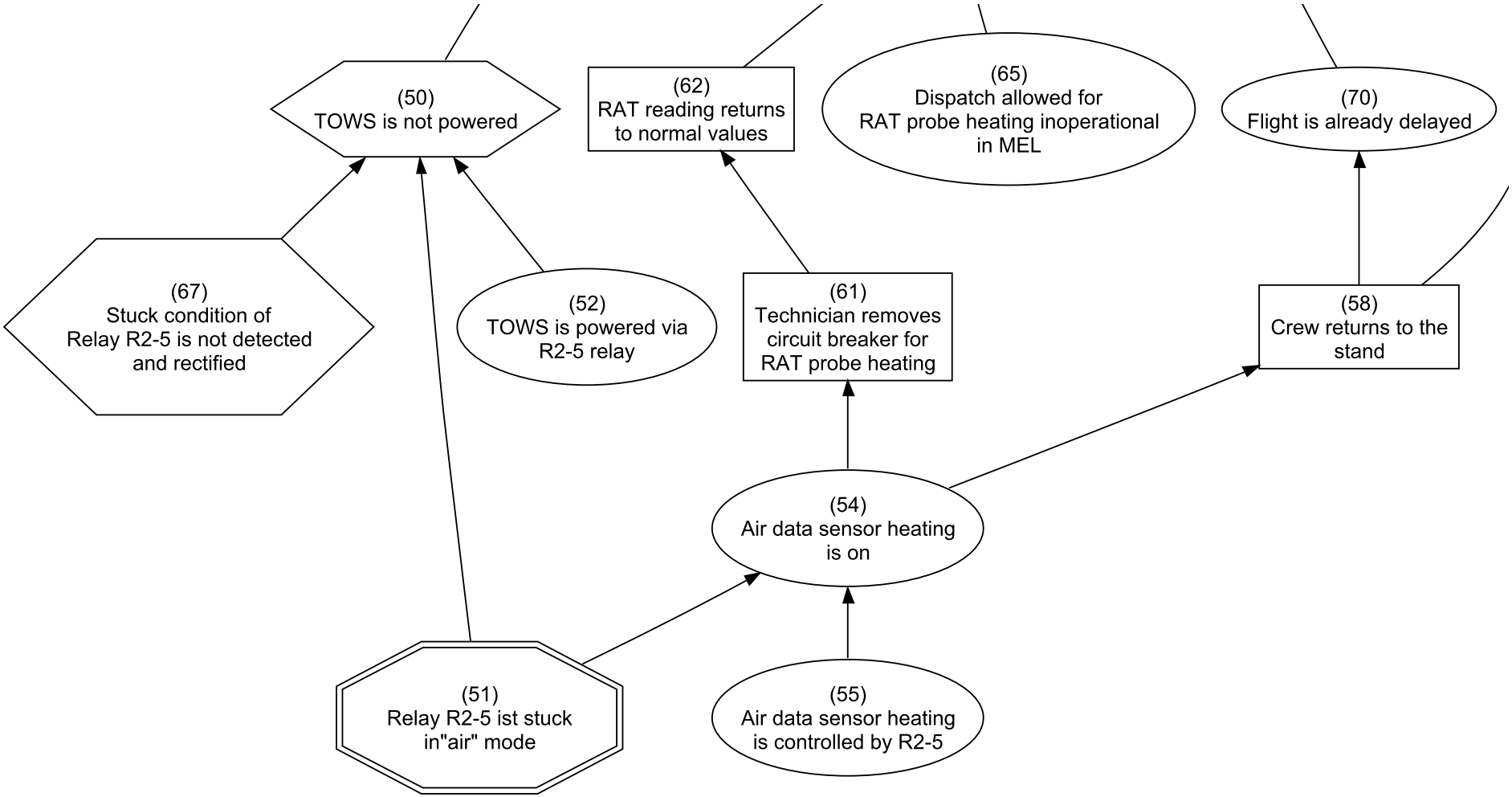


- Relays to switch various devices from ground-mode to air-mode
- Relay R2-5 probably 'stuck' in air-mode
- R2-5 switches RAT-probe heat and Takeoff-Warning System (TOWS)
- TOWS inhibited in the air
- RAT-probe heater CB pulled
- $\Rightarrow$ RAT-probe ok
- $\Rightarrow$ TOWS inoperative
- Next Takeoff attempt with retracted Flaps

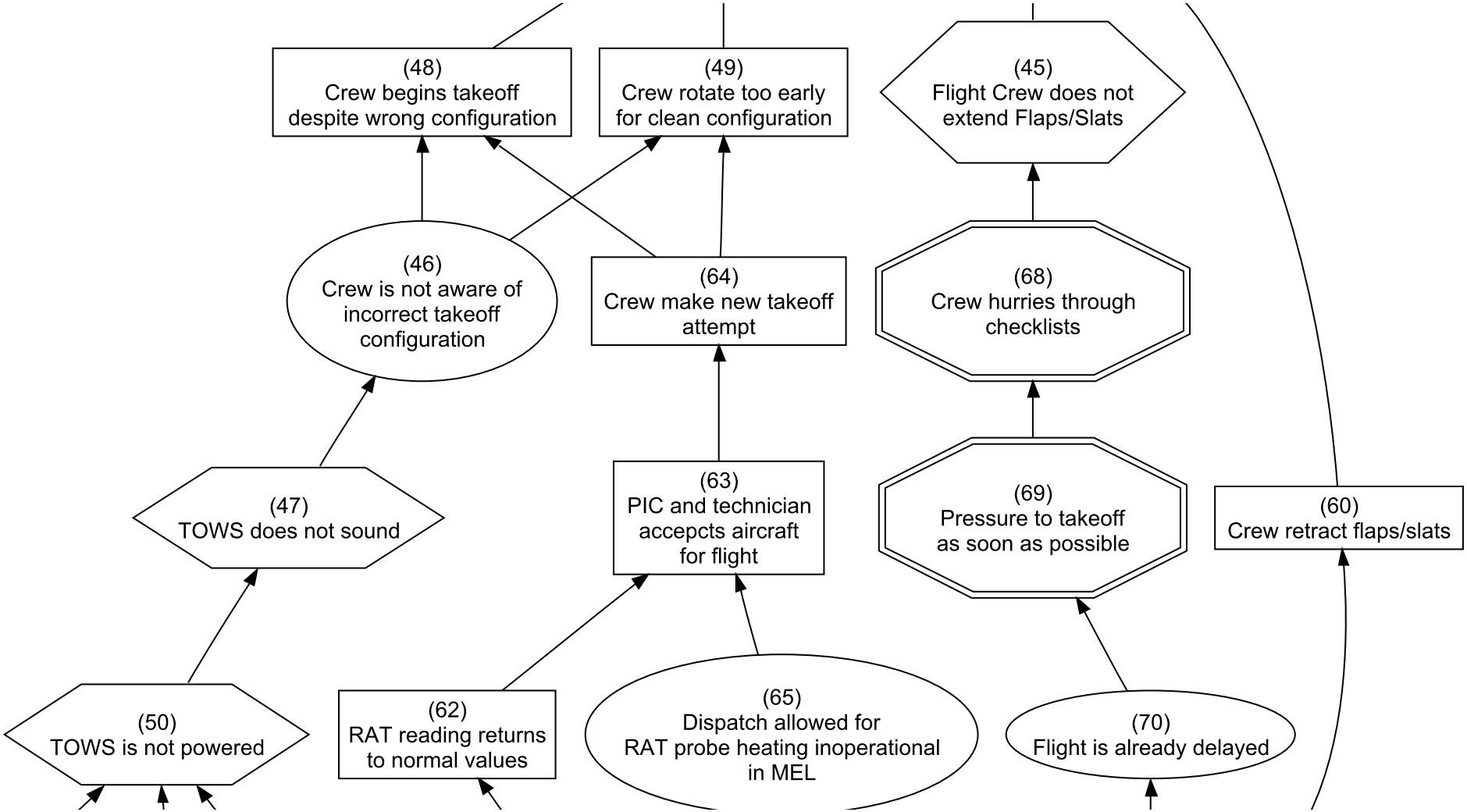
Spanair Accident — Why-Because Graph



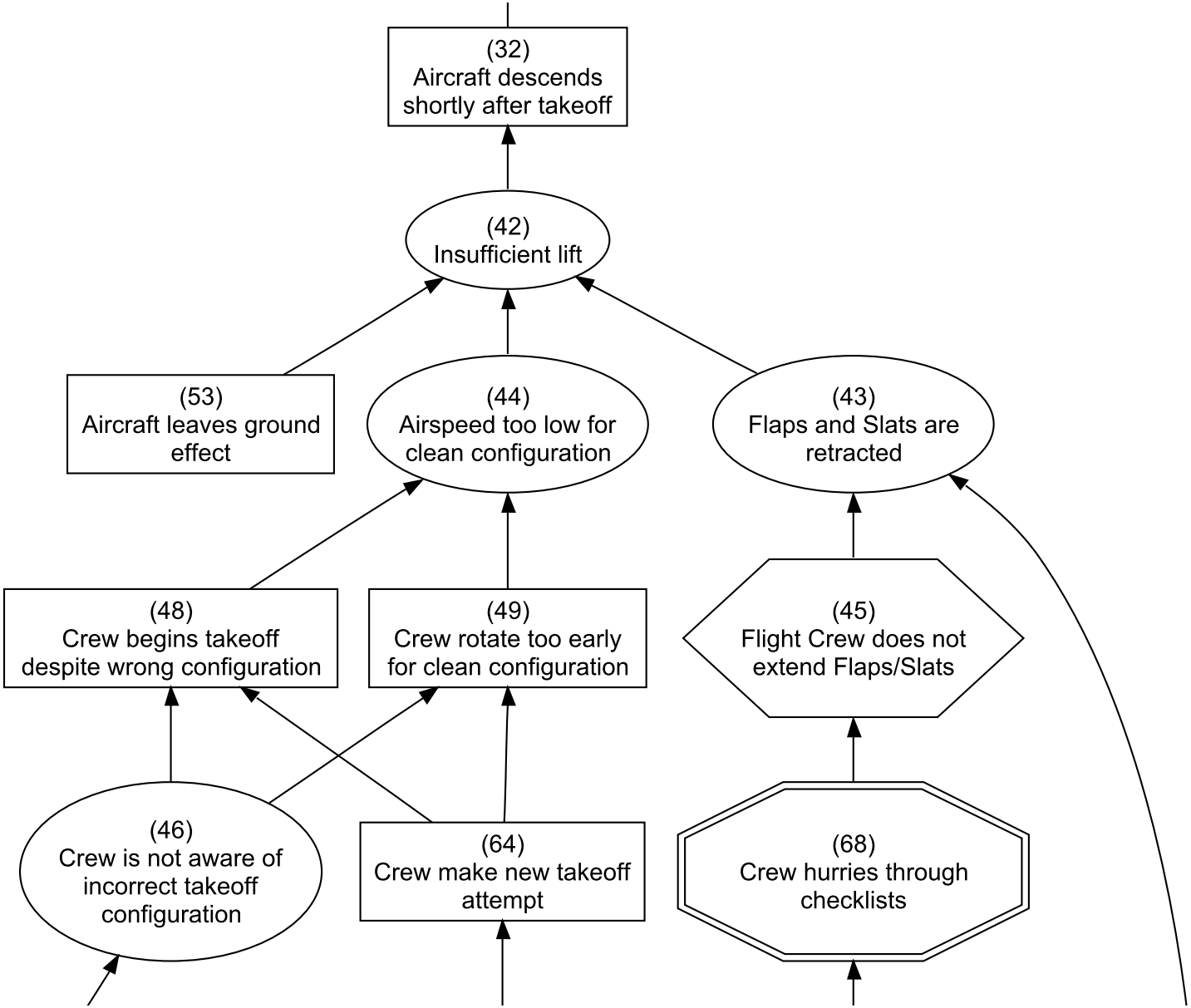
Spanair Accident — WBG Lower Part



Spanair Accident — WBG Middle Part



Spanair Accident — WBG Uppper Part



Spanair Accident — Lessons learned?

Many cases of "Duh! That was obvious ..."

Well, they happened anyway, so let's take a look.

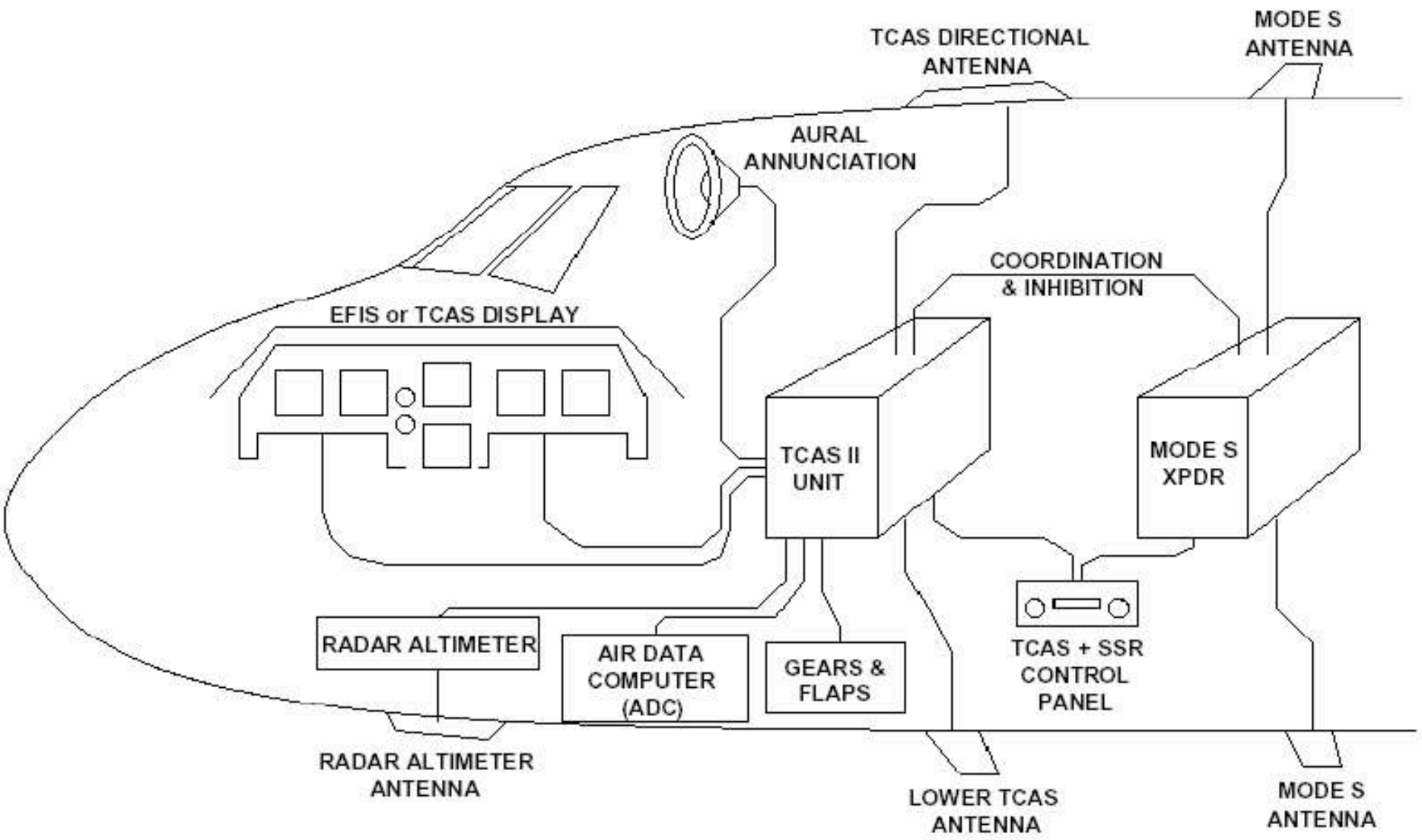
- Don't takeoff at low speeds without flaps
- Respect the Stall Warning / Stick Shaker[2]
- *Do Not Rely on the Automatics to Save You*
- Investigate the reasons for any Malfunction
- Be sure to understand Manuals (MEL)

[2] Also see recent C-17 accident

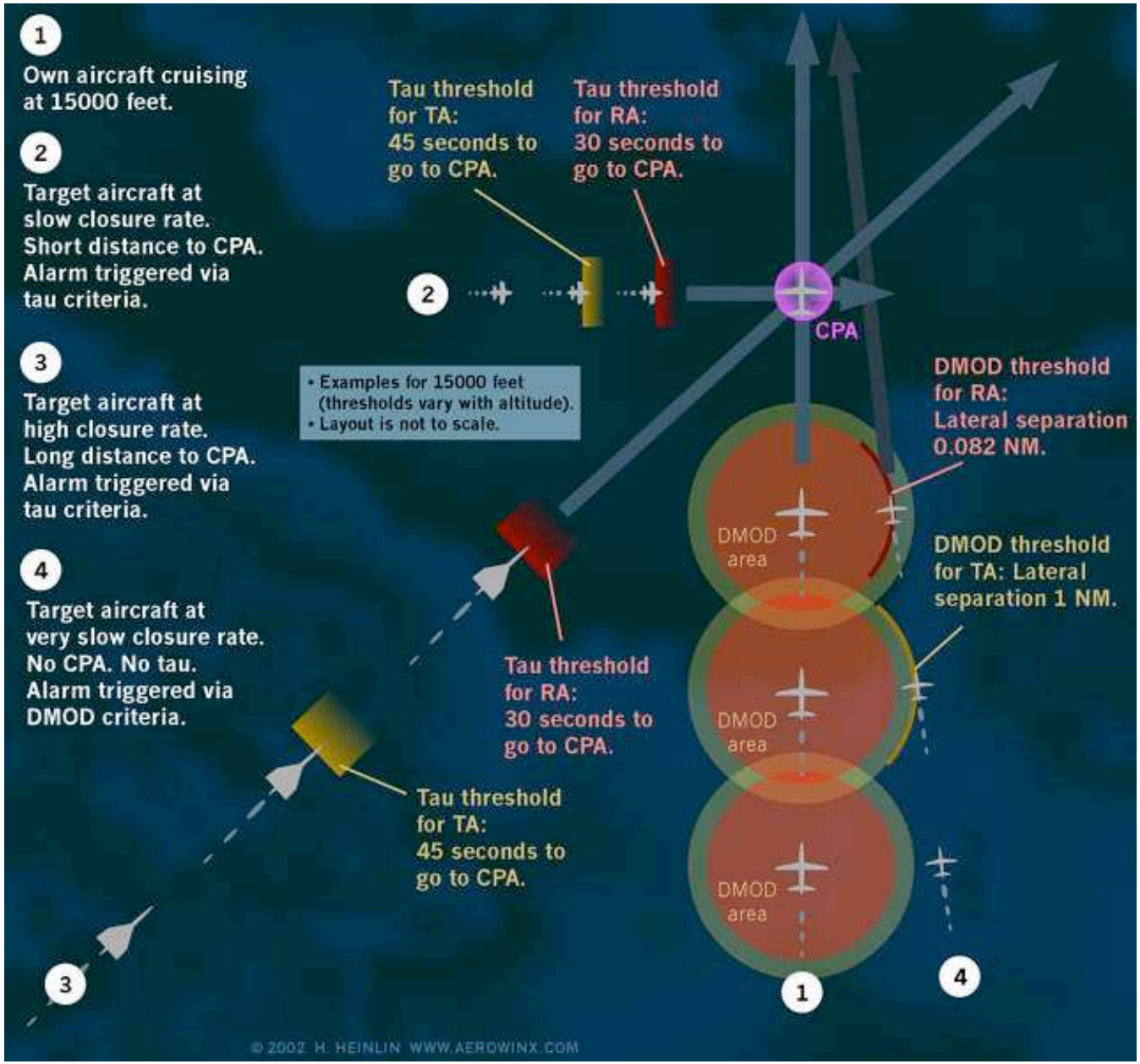
Rational Cognitive Models — TCAS and the Überlingen Midair Collision

- Two airliners (Tu-154, B757) on intersecting trajectories at roughly right angles
- Both equipped with on-board collision avoidance system (ACAS/TCAS)
- Air traffic controller realises situation late (though not strictly too late)
- ATC mistake alerting one crew of conflicting traffic
- Tupolev 154: instructed by ATC to descend, by TCAS to climb
- Boeing 757 instructed by TCAS to descend
- Both airplanes descend and collide.
- Both airplanes are destroyed, all occupants die

The TCAS "kit"


TCAS DIRECTIONAL ANTENNA
MODE S ANTENNA
AURAL ANNUNCIATION
COORDINATION & INHIBITION
EFIS or TCAS DISPLAY
TCAS II UNIT
MODE S XPDR
RADAR ALTIMETER
AIR DATA COMPUTER (ADC)
GEARS & FLAPS
TCAS + SSR CONTROL PANEL
RADAR ALTIMETER ANTENNA
LOWER TCAS ANTENNA
MODE S ANTENNA

TCAS Criteria



Überlingen Mid-Air Collision

First State

DHL

- Conflict
- We descend
- **X** Other likely climbing

Bashkirian

- TCAS Conflict
- **X** Other Conflict (unknown, non-TCAS)
- TCAS traffic in sight
- other traffic not seen
- → We descend

Controller

- **X** DHL at FL 360
- Bashkirian at FL 360 and descending

Überlingen Mid-Air Collision

Second State

DHL

- State unchanged

Bashkirian

- State unchanged

Controller

- State change
  DHL TCAS escape manœuvre

Überlingen Mid-Air Collision

Third State

DHL

- !Collision!

Bashkirian

- !Collision!

Controller

- Blank radar screen

The TCAS system — Boundaries?

What is the TCAS system?

- The "kit"?
- Kit + Crew?
- Kit + Crwe + Crew?
- Kit + Crew + Crew + ATC?

Design Principles for Interactive Systems

Rational Cognitive Model Coherence All participants must maintain mutually coherent "views" of the state of the world
Violated: Conflicting "views" of both aircarft's states

Bounded-Rationality Criterion There shall arise no state in which a safety-related decision to be taken requires more rational capabilities than are available to the agent

Mutual Cognisance of Relevant Parameters All participants must "know" about all parameters, knowledge of which is required to achieve a specific goal.
Violated: ATC has no way of knowing aircraft manœuvres immediately

Procedural Completeness For every reachable state there is an explicit procedure for every agent involved in the task.
Violated: There is no procedure for conflicting instructions from ATC and TCAS

TCAS specifications ...

- TCAS technical system performed to specifications
- Reversal Resolution Advisory not specified for situation at Überlingen
- Problem was known: Change proposals had been filed since before the accident
- Yes, it performed to spec, but the specs were flawed

Conclusions?

It's not quite that easy ...

- Automation can be problematic
  - Overreliance on Automation may lead to complacency
  - Amount and way of presentation is a non-trivial design challenge
- on the other hand, when all goes well, ...
  - Automation reduces crew workload
  - Can make manœuvres possible that are impossible without it (Video)

Conclusions? -2-

- Qantas Flight 32

  - Airbus A380
  - Uncontained engine failure: “liberated” turbine disk
  - Severe damage to left wing; Control of other left engine lost
  - Crew spent $>$ 1h to process ECAM messages
  - $\Rightarrow$ Crew had exhaustive knowledge of failed systems
  - $\Rightarrow$ Crew could make informced decision for landing procedures

Conclusions? -3-

- NTSB study[3]:

(Left Photo: thatguyeric[4])

  - Lower total accident rate
  - Higher fatal accident rate
  - Possibly because of different layout and failure modes
  - “steam” gauges are almost always the same

[3] http://www.ntsb.gov/pressrel/2010/100309.html
[4] http://www.flickr.com/people/thatguyeric/

Conclusions? -4-

- Automation can help enormouslay
- Automation is no subsitute for a well-trained crew
- Proper use of the correct level of automation must be trained

The End

Thank you very much for your attention!

Questions? Comments?