The Causal Analysis of Sociotechnical Systems

I: The Avionics System ACAS/TCAS

Peter B. Ladkin
ladkin@rvs.uni-bielefeld.de

Contents

- Characteristics of Avionics Systems
- ACAS & TCAS: Technology
- ACAS Manoeuvres and Operation
- The Role of Air Traffic Control (ATC)
- The Midair Collision over Überlingen
- Two Observations on Causality and System Interaction
- Seven Issues
  - Issue 1: Faulty System Requirements
  - Issue 2: ACAS in the RVSM Environment
  - Issue 3: ACAS Algorithm Correctness
Contents (cont’d)

- Issue 4: Conflicting Advice on TCAS Use
- Issue 5: Operator Cognitive State
- Issue 6: What Components Has the ACAS System?
- Issue 7: ACAS System State
- Conclusions Concerning These Issues
- Comments on Causal Reasoning
- Conclusion and Acknowledgements

Avionics Systems

- Few are critical control systems
  - The (one or many) Flight Control System(s)
  - Full-authority digital engine control (FADEC)
- Most are flight-aiding systems
  - Flight Management System for navigation
  - Data systems
    - Fuel management
    - “Air data”: airspeed, altitude data delivery and so on
  - Climate control and passenger systems
    - Air conditioning
    - Anti-ice
    - Pressurisation
    - In-flight entertainment
Many of the aiding systems are not officially regarded as “safety-critical” (except for Air Data Systems)

However, such systems and their use have been one of the main causes of accidents
- Strasbourg 1992
- Toulouse 1994
- Cali 1995
- Puerto Plata 1996
- Lima 1996
- Taipei 1998
- ... and so on
Avionics Systems

- Many of these systems do not “degrade gracefully”
  - Airspeed data: precision required by FCS
  - Altitude data: precision required by RVSM, also by approach and landing systems
  - Navigation data: accuracy required on descent in mountainous terrain, and on every approach
- How could a system “gracefully degrade” in the event of pitot-static sensor blocking (Puerto Plata, Lima)?

Flight Control Systems

- Apart from some early anomalies, there have not been commercial aviation accidents in which failure of digital flight control systems (DFCSs) has played a significant role
  - Habsheim 1988? Mostly caused by inadequate flight planning and execution
  - Warsaw 1993? Some unavoidable physical constraints, but braking systems actuation criteria were modified afterwards nonetheless
  - Dragonair Hong Kong incident 1994. Flaps locked in place due to turbulence, FCS sensed false position
  - Frankfurt 2001. Maintenance error – wired wrong
Avionics Systems as Socio-Technical

- Socio-technical (sociotech) systems are those which have technical components as well as human-group components

- Many cockpit systems are sociotech
  - Cockpit crew (CRW) is a social entity
    - Crew Resource Management (CRM)
    - Line-Oriented Flight Training (LOFT)
  - The avionics is advisory, CRW is the executor
    - Flight management
    - Systems management including failure
    - ACAS/TCAS

ACAS & TCAS: Technology
ACAS & TCAS: Nomenclature

- ACAS II is an International Civil Aviation Organisation (ICAO) specification for an Airborne Collision Avoidance System
- TCAS is the U.S. name for such a system, developed in the U.S. by inter alia Mitre and Honeywell
- Honeywell and ACSS are main providers of ACAS avionics (kit), with TCAS II V6.04a and TCAS II V7.0 flying
- Note:
  - TCAS II V7.0 is ACAS II compliant
  - TCAS II V6.04a is not ACAS II compliant
- I refer to the system as ACAS, the kit as TCAS

ACAS as a SocioTech System

- ACAS avionics is purely advisory
  - There is no link between ACAS/TCAS and any flight control or autopilot systems
- CRW must take action
  - Both Pilot Flying (PF) and Pilot Not Flying (PNF) have important roles, as we shall see
  - There is a Pilot in Command (PIC)
- CRW acts according to PIC discretion – the predominant legal principle of flight
ACAS Technology

- ACAS II is required in EUR-Airspace since Jan 2000, with a transition period until Mar 2001
- Reminder: Honeywell main provider, TCAS II
  - V6.04a in use: not ACAS II-compliant
  - V7 available since late 2000
- TCAS works from transmitted altitude data, and from horizontal closing-rate data
- TCAS warns of other aircraft in the immediate vicinity (Traffic Advisory, TA)
- TCAS advises an avoidance manoeuvre (Resolution Advisory, RA) if “intruder” close

From Eurocontrol’s ACAS II Training Manual
ACAS Technology: Displays

- A display screen provides a plan view, and highlights the position of "intruders"
- Positional information is only approximate
- Advisories are visual (highlighted screen) and aural (synthesised voice)
- Two levels of advisory:
  - Traffic Advisory (TA). Vigilance expected
  - Resolution Advisory (RA). Manoeuvre expected

TCAS "Classical" Display

- From Eurocontrol’s ACAS II Training Manual
TCAS Display in "Glass" Cockpits

- From Eurocontrol's ACAS II Training Manual
ACAS Resolution Advisory (RA)

- RAs are vertical-sense only ("Climb", "Descend")
- RA issued within an "alert threshold" based on predicted "time to go" (ttg) before collision
- Two-level ("climb", "increase climb") based on 1,500 fpm, resp. 2,500 fpm vertical speed
- Iterative (two consecutive RAs may be issued)
  - strengthening: "climb", "increase climb"
  - constant: "climb", "maintain vertical speed"
  - weakening: "climb", "adjust vertical speed"
  - reversing: "climb", "descend NOW"

RA Display on the IVSI

- Descend
- Climb
- Adjust vertical speed (weakening advisory)
- Increase climb (strengthening advisory)
- Maintain vertical speed (maintain climb)
- Adjust vertical speed (reduce rate of descent)
- Adjust vertical speed (multi-threat advisory)
- Monitor vertical speed
To simplify, consider the case of constant relative velocity

I consider first a simple criterion

Two converging aircraft have geometrically a “closest point of approach” (CPA), at which the horizontal distance \( d(\text{CPA}) \) between them will be minimal

This occurs at a particular time in the future: \( t(\text{CPA}) \)

“time to go” \( ttg = t(\text{CPA}) - t(\text{now}) \)

Suppose the horizontal distance \( d(\text{CPA}) \) and vertical distance \( z(\text{CPA}) \) will each be below a threshold

Then one would like to warn both aircraft in enough time (say, 35 seconds) to allow gentle manoeuvring to change the situation

Instead, a composite measure is used, called \( \tau(\text{Tau}) \), whose units are seconds:

\[ \tau = \frac{\text{(relative range of aircraft)}}{\text{(closure rate)}} \]

Note \( \tau \) will be larger than \( ttg \) if \( d(\text{CPA}) > 0 \)

TA and RA triggering is based upon \( \tau \), for example

- 5000 AGL Radar Altitude – FL 100
  - TA threshold: \( \tau = 40 \) sec; RA threshold: \( \tau = 25 \) sec
- FL 100-199:
  - TA threshold: \( \tau = 45 \) sec; RA threshold: \( \tau = 30 \) sec
- FL 200 upwards:
  - TA threshold: \( \tau = 48 \) sec; RA threshold: \( \tau = 35 \) sec

\( \tau \) is used in combination with \( z(\text{CPA}) \) threshold \( Z\text{THR} \)
The Tau Criterion: DMOD

- In the case of slow rates of closure (say, the aircraft are travelling almost parallel), using the raw $\tau$ might allow the aircraft to approach quite closely in the horizontal plane before an advisory is generated.

- An additional criterion, the horizontal separation DMOD, also triggers advisories:
  - FL 050 – FL 100
    - TA threshold: 0.75nm (nautical miles); RA threshold: 0.55nm
  - FL 100-199:
    - TA threshold: 1nm; RA threshold: 0.8nm
  - FL 200 upwards:
    - TA threshold: 1.3nm; RA threshold: 1.1nm

ACAS $\tau$: Protected Area Illustration
Incursion into Protected Volume

- Avoidance manoeuvres negotiated between aircraft
  - One receives "climb" RA, the other "descend" RA
  - RAs normally conform to altitude differences
    - The higher aircraft receives a "climb" RA, the lower a "descend"
- ...... but must not: so-called "crossing RAs"
  - "climb, crossing climb"

Other Tau Criteria

- More sophisticated criteria have been considered, such as Modified, which takes acceleration into account, and Range Test
- Also three-dimensional manoeuvring has been considered in research. Practical problems would be
  - Manoeuvring in the vertical plane is more rapidly achieved than in the horizontal
  - Manoeuvring commands would be no longer cognitively simple, and simple is better
  - Air traffic control (ATC) is based on separate horizontal and vertical separation. Vertical manoeuvres affect just one parameter and are cognitively simple for ATC. Affecting both would increase cognitive complexity for ATC, who may have to react by separating non-involved traffic to prevent a "chain reaction"
ACAS Operation and Manoeuvres

Standard Manoeuvre

- From Eurocontrol's ACAS II Training Manual
The sense is selected according to which predicted vertical separation is larger. In this case, B is larger: TCAS issues a "descend, descend" RA.

From Eurocontrol's ACAS II Training Manual

ALIM is desired vertical separation. If ALIM is predicted to be achieved by so doing, higher aircraft will be issued a climb RA, else a "crossing" manoeuvre will be instigated (a descend RA for the higher aircraft).

From Eurocontrol's ACAS II Training Manual
A second advisory may be issued in cases in which the prediction on which the first is based will not be achieved, for example through a manoeuvre by the "threat": here, an increased rate of descent is advised (to 2,500 fpm from 1,500 fpm)

From Eurocontrol’s ACAS II Training Manual

In certain circumstances, an initial RA may be reversed by the second RA. Here, an initial climb RA is changed to a descend RA ("descend, descend now") in response to a manoeuvre by the "threat"

From Eurocontrol's ACAS II Training Manual
RA and Iterated RA Notification

- RAs and iterated RAs are announced by a specific form of words for each case:
  - initial corrective RA: “climb, climb”
  - strengthening iterated RA: “increase climb, increase climb”
  - weakening iterated RA: “adjust vertical speed, adjust”
  - reversal RA: “descend, descend NOW”
  - RA with altitude crossing: “climb, crossing climb, climb, crossing climb”
  - iterated RA to maintain vertical speed: “maintain vertical speed, maintain”
  - Etc

The Role of Air Traffic Control (ATC)
Aircraft at FL 290 - FL 410 (as well as other flight levels) are under "positive control"

That is, airspace is "cleared" for them by ATC, which guarantees that no other aircraft will be in the cleared airspace

Clearances are both long-range (at start) and dynamic (aircraft entering a controller's range will be given modified clearances to avoid other aircraft already under hisher control)

The assumption ("principle") is that an RA is a "last-minute" manoeuvre

it is issued at what is regarded as the last possible moment for avoidance according to the separation and manueuvring parameters

it is assumed or inferred that an RA will only be issued when ATC separation has failed
ATC Procedures During Notified RA (2)

- ATC has specific responsibility during an RA manoeuvre
  - During an RA manoeuvre, ATC is no longer responsible for separation of aircraft until “Clear of Conflict” is announced. ATC function is restricted to issuing positional advisories only
  - ATC must be verbally notified by CRW of an RA manoeuvre (“RA climb”/“RA descent”), and verbally notified by CRW of its end (“Clear of Conflict”)
  - ATC does not know of an RA until verbally notified
  - This allows for a time lag in common understanding of the situation between ATC and CRW

ATC and CRW Interaction During RA

- An argument has been generally accepted that
  - because an RA is only triggered if ATC separation has definitively failed, ATC plays no further role in the proceedings until “Clear of Conflict” announced
  - Therefore ATC plays no further causal role in interactions during RA manoeuvres

- This argument is unfortunately invalid
  - In the Überlingen incident, an ATC informational slip altered one participant's understanding of the situation and allowed a decision which was rational in the misunderstood situation, but not in the actual one, as we shall see (Issue 5, below)
An Unresolved Issue

- ATC clears airspace
- Following an ACAS RA, an aircraft departs from cleared airspace
- The airspace into which the manoeuvring aircraft enter may not be clear for them
  - Following an RA may induce a further risk of collision with other traffic, and hence further RAs
  - One hopes such "chain reactions" will not happen - but they have, e.g., Trasadingen, Switzerland, 13 Sept. 2000
- The vertical volume of cleared airspace at altitude (FL 290 – FL 410) under Reduced Vertical Separation Minima (RVSM) is half what it used to be under conventional separation

The Midair Collision Over Überlingen
Lake Constance Midair (1)

- 1 July, 2002 over Lake Constance, S Germany
  - AC under control of Zürich ATC
    - Same controller, same frequency
  - DHL 611 northbound, in contact for 13+ minutes
  - BTC 2937 westbound, in contact for 4+ minutes
  - Both at FL 360 initially

Map of Überlingen Collision
Lake Constance Midair (2)

- TCAS TA received by both aircraft
- 7 seconds later, BTC received ATC advisory to descend "expedite" for traffic. PIC gives immediate descent command. At end of ATC advisory, TCAS RA issued to climb.
- At about same time, DHL receives "descend" RA
- 7 seconds later, ATC repeats descent advisory, advises of traffic at "2 o'clock". DHL is at 10 o'clock. BTC searches for traffic at 2 o'clock as well as at 10 o'clock.

Lake Constance Midair (3)

- 7 seconds later, DHL receives strengthened RA "increase descent"
- 9 seconds later, DHL advises ATC of TCAS descent. Announcement delayed because PF was performing all duties until PNF returned to right seat
- 5 seconds later BTC receives strengthened RA "increase climb" (14 seconds after DHL's 2nd RA!)
- 6 seconds later, they collide
Reconstructed Collision

Collision Angles from a Plan View
Two Observations on Causality and System Interaction

First Observation

- Use of the ACAS system was a causal factor in the accident chain

- Proof:
  Use the Counterfactual Test

  - DHL and BTC collided at about FL 350
  - Had DHL not descended, BTC and DHL would not have collided
  - DHL would not have descended,
    - had ACAS avionics not been installed, or
    - had the RA not been followed by DHL's CRW

  QED
Second Observation

- ACAS use alone would have avoided the collision
- ATC advisories alone would have avoided the collision –
  - the aircraft would have missed each other by 1000+ vertical feet - collision was at “34,890 ft altitude”
- But their concurrent use was in this case fatal
- Conclusion: ACAS and ATC subsystem interaction is safety-critical

Seven Issues
Issue 1: Faulty Requirements

- It is hard to imagine a situation more appropriate for a Reversal-RA
  - Both aircraft were descending in parallel, and converging horizontally at ~700 kts = ~1300 kph

- BFU determined that the requirements for a Reversal-RA to be issued were not fulfilled

- Conclusion: the requirement specification is inadequate to the real requirement
  - This was not remarked in the BFU report
Issue 2: ACAS in the RVSM Environment

What is RVSM?

- From FL 290 to FL 420, aircraft under conventional vertical separation minima (CVSM) were assigned flight levels in 2,000 ft increments (that is, FL 310, FL 330, FL 350, FL 370, ..)

- Under Reduced VSM (RVSM), flight levels are now assigned at these altitudes in 1,000 ft increments (FL 300, FL 310, FL 320, FL 330, ..)

- Aircraft may now legitimately pass each other in cruising flight with only 1,000 ft nominal vertical separation

- That leaves much less room vertically to manoeuvre (and recover) in response to an ACAS RA
Eurocontrol claims concerning the Safety Case for RVSM that their ACASA project, which studied aspects of ACAS use in European airspace, identified no safety issues with ACAS and RVSM, and that therefore the Safety Case could be made without considering interactions with ACAS

I disagree. See “The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed” under www.rvs.uni-bielefeld.de

I claim the interactions between ACAS and RVSM have been inadequately studied

There are interactions

- Interaction not only through valid RAs (this accident)
- But also interaction through spurious RAs
  - TRA incident: on 13 September 2000, a four-aircraft chain reaction in the vicinity of the Trasadingen VOR (TRA) occurred. The lowest aircraft was climbing fast to reach assigned altitude. A spurious RA was triggered in the next-highest aircraft, whose climb triggered an RA in the third, which in turn triggered one in the fourth, who filed an airprox report with the Swiss authorities.
  - Turbulence: on 2 October 2000, an encounter with unexpected turbulence (a “bump”) on North Atlantic Track E (NAT E) initiated a “balloon climb” of an A340 through the altitude of an A330 following in trail under RVSM. The A330 commander had no time to react to the TCAS RA. Horizontal separation was 200-300 ft.

Risk can be increased by RAs

Interaction through spurious RAs can increase risk over that without ACAS (incident at TRA, 13.09.2000)

So can multi-aircraft interaction triggered by a valid RA increase risk, if it sets forth a chain reaction
The ACASA Project

- Potential interactions between ACAS and RVSM were studied by the Eurocontrol ACASA project
  - Statistical tests were performed, based on massaged radar data from actual operations
  - No significant ACAS/RVSM interaction issues were identified
  - Days of radar data were used. But legitimately to draw a conclusion that there are no significant interactions at the set Target Level of Safety, it would have been necessary to use decades, or hundreds of years, of data (follows from a basic observation by Littlewood & Strigini, 1993)
  - A discrete analysis, taking into account the possibilities shown by the TRA and NAT E incidents, was not performed

Risk (1)

- Risk can be increased by RAs under RVSM
  - Interaction through spurious RAs can increase risk over that without ACAS (incident at TRA, 13.09.2000)
  - So can multi-aircraft interaction triggered by a valid RA increase risk, if it sets forth a chain reaction
  - There is a much reduced buffer for excursions:
    - an avoidance manoeuvre, when correctly executed (by no means always the case):
      - 2 secs reaction time, ¼ g manoeuvre to 1500 fpm: acceleration takes 3.125 sec and 39 vertical feet; thereafter 38 seconds to 1000 ft above initial altitude. Total 43 seconds.
      - same initial dynamics; thereafter 78 seconds to 2000 ft above initial altitude. Total 83 seconds
      - The extra 1000 ft under CVSM allows 40 secs longer for a standard manoeuvre until possible secondary conflict. Abrupt manoeuvring reduces these times
Risk (2)

- Risk can also be increased by TAs under RVSM
  - Two aircraft passing each other at 1,000 ft vertical separation, one with TCAS V6.04a
    - TA
      - TA requires monitoring from CRW according to procedure
      - Monitoring a spurious TA diverts attention away from other tasks
      - Diverting attention from non-spurious tasks increases the risk that they will not be attended to properly
    - This is a recognised issue, dealt with by assuming minimal and decreasing use of V6.04a in EUR-RVSM airspace

Expected rates (actual & spurious)

- TCAS II V7.0, TA
  - 1 TA every 20 flight hours in RVSM (above FL290)
  - 60 CVSM
  - 5 FL250-FL290

- TCAS II V7.0, RA
  - 1 RA every 330 flight hours in RVSM (above FL290)
  - 1000 CVSM
  - 70 FL250-FL290

- TCAS II V6.04a data much worse -> “operational issue”

ACAS in RVSM. The Ideal Case

TCAS V7.0 issues a TA at 850 ft perceived vertical separation (pvs)
TCAS V6.04a issues a TA at 1,200 ft pvs: an “issue”

TCAS and RVSM: The Ideal Case

- TCAS V7.0
  - TA at 850 ft perceived vertical separation (pvs)
  - RA at 700 ft pvs

- TCAS V6.04a
  - TA at 1,200 ft pvs: an “issue” in RVSM
  - RA at 800 ft
Spurious Advisories in RVSM

- Maximum allowed FL offset 65 ft
- Altitude reporting in 100-ft increments (can also be 25-ft increments)
- Aircraft can "see" each other at < 850 ft separation
  - Aircraft A at FL 340 but 51 ft low
  - Aircraft A reports at FL 339 (100-ft increment)
  - Aircraft B TCAS "sees" AC A at FL 339
  - Aircraft B at FL 330 but 51 ft high
  - TCAS calculates relative altitude 849 ft
  - TA is generated even with V7.0
- RA not generated by either version V6.04a or V7.0
Autopilots are feedback control systems, and, as with any such systems, they can oscillate about their target value. Analysis of this case similar to that of previous.

A “bump” due to turbulence imparts a sudden acceleration to the aircraft, which registers as the start of a climb manoeuvre. If there are vertically adjacent aircraft, an RA may be triggered by the sudden acceleration. As indeed it was by the NAT E October 2000 incident.
Issues Are Known

- These issues are known; indeed, the examples are taken from Eurocontrol's ACAS II Training Manual
- Nevertheless, they are argued to be sufficiently rare
- But without appropriate statistical calculations of their rarity
- Conclusion: the issues remain

Spurious Advisories

- With TCAS II V7.0, only spurious TAs are generated near the limits of allowed error
- RAs are generated at 700ft annunciated-altitude difference
- However, RAs may be generated through turbulence encounters, as well as through pilots not maintaining precision altitude while hand-flying (rare)
Issue 3: ACAS Algorithm Correctness

- Eurocontrol ACAS II Training Manual:
  - “TCAS is able to handle multi-threat situations either by attempting to resolve the situation with a single RA, which will maintain safe vertical distance from each of the threat aircraft, or by selecting an RA that is a composite of non-contradictory climb and descend restrictions.”
  - “TCAS significantly improves flight safety. However, it cannot entirely eliminate all risks of collision. Additionally, as in any predictive system, it might itself induce a risk of collision”
Three Aircraft Conflicts

- In August 2002, I classified three-aircraft conflicts into a number of classes with similar conflict geometry for the TCAS algorithms.
- Most were resolved through sequential RAs, using the TCAS qualitative logic.
- I identified one situation which was not resolved using TCAS qualitative logic. I asked around. The issue remains open whether this configuration is always resolved, or whether there is a non-resolution example. It requires quantitative geometric reasoning.

"ACAS and the South German Midair", RVS-RR-02-02, available at www.rvs.uni-bielefeld.de
### Three-Aircraft Conflict: Example 1

- Aircraft A and B converge at Flight Level L
- An RA is issued, requiring B to climb and A to descend
- C is descending towards B; I assume that a non-crossing RA cannot be issued; a crossing RA is issued
- C descends towards A at 1,500 fpm
- A is already descending at 1,500 fpm
- ACAS can handle convergence rates of 1,200 kts and 10,000 fpm
- ACAS then handles A and C without problem

### Three-Aircraft Conflict: Example 2

- Consider now the case in which aircraft A and C are already within the alert threshold at the time at which the crossing RA to aircraft B and C is issued
- Is this resolved?
- This remains an open problem
Situation 3: Resolution? Unknown

Multiple Aircraft in General (Kuchar)

This example is due to Jim Kuchar of MIT Lincoln Labs.
ACAS for Multiple Aircraft

- TCAS can resolve all two-aircraft conflicts (Nancy Lynch, John Lygeros, Carolas Livadas, 1999)

- General multi-aircraft avoidance requires alerting before that given by a pairwise-resolution algorithm such as TCAS (Jim Kuchar, Lee Yang, 1997)

- What is the smallest number of aircraft for which simultaneous conflict cannot be resolved by TCAS?

- It is possible that the answer is 3 aircraft

- BTC believed it was in a 3-aircraft conflict

Issue 4: Conflicting Advice on TCAS Use
Conflicting Advice

- The BFU accident report contains a thorough investigation of the different advice from different quarters on procedures concerning RAs.
- I summarise.

Issue 4: Conflicting Advice on TCAS Use

- Eurocontrol literature advises pilots always to follow an RA.
- ICAO Annex 2, Ch.3, 3.2.2 position is that nothing relieves a PIC of responsibility from taking whatever manoeuvring action as will best avoid a collision.
- ICAO Annex 10 Attachment A para 3.5.8.10.3 says that manoeuvres opposite to the sense of an RA must be avoided.
- ICAO Doc 8186, PANS-OPS Ch 3, 3.1.1 says that ACAS info is intended to assist pilots in the operation of aircraft.
- ICAO PANS-OPS 3.1.2 says that nothing specified in 3.2 (manoeuvring in response to TA/RAs) shall prevent PICs from exercising best judgement and full authority in the choice of a course of action to resolve a traffic conflict.
Conflicting Advice (2)

- JAA Leaflet 11, Oct 1998, 3.2.36 Note 3 says that if pilots simultaneously receive conflicting ATC and RA manoeuvre instructions, the pilot should follow the RA.

- UK CAA position is also "should" rather than "shall". They say: "...to allow for Commander's discretion to cater for those very limited cases where use of such discretion avoids an incident where the following of ACAS advice may make matters worse".

- Luftfahrhandbuch Deutschland (AIP Germany) 2.2.2a says that all RAs should be followed, except when the PIC can visually identify the intruder and decides that no deviation from current flightpath is necessary.

Conflicting Advice (3)

- LuftVO (Rules of the Air) §13 Abs. 9 says that the requirements concerning avoidance manoeuvres, including RA manoeuvres, do not release the PIC from the obligation to conduct the flight to avoid collision.

- FAA AC 120-55B, 22.10.2001 11.b(2) says that the PF should manoeuvre as indicated by an RA unless doing so would jeopardise the safe operation of the flight, or CRW can assure separation through definitive visual acquisition of the intruder.

- The TU154M Operations Manual 6.12.1999, 8.18.3.4 says that the main means to prevent in-flight collision are visual control of the situation by the CRW and following ATC instructions. TCAS is an additional means that enables identification of conflicting traffic, classification of the hazard, and, if necessary, following a command through initiation of a vertical manoeuvre.
Conflicting Advice (4)

- The BFU position is that following an RA should be mandatory.
- This is a radical position.
  - To date in the history of aviation, no specific manoeuvre is mandated of aircraft commanders.
  - Aircraft commanders are to decide on manoeuvres using the criterion of the safety of the aircraft and its occupants, taking the situation into account.
- It is also highly questionable.
  - Mandate a manoeuvre which belongs to an algorithm whose correctness is not known for three-aircraft conflicts?
  - BFU suggests it must always be the best decision.
  - But BTC believed they were in a three-aircraft conflict.

Issue 5: Operator Cognitive State:
The Decision to Descend
Issue 5: Operator cognitive state (BTC)

- TA (traffic approx. position displayed)
- ATC advisory to descend, "expedite" for traffic
- RA to climb (traffic displayed at 10 o'clock)
- Second ATC advisory to descend for traffic at "2 o'clock"
- Cognitive situation: One target you "see"; one target you don't see
- Decision?

BTC's Manoeuvring Decision (1)

- Observe (1):
  - (1) crudely: there is no possible decision for BTC consistent with all their required procedures
    - “Follow the RA”
      - Eurocontrol (thereby Russian training) says follow the RA
      - JAA leaflet 11 says in case of simultaneously conflicting ATC advisory and an RA follow the RA
    - “Need not follow the RA, but don't go against”
      - AIP Germany says never to manoeuvre against an RA if it is decided not to follow it, and you many not follow an RA if you have visually acquired the intruder and decided that no deviation is needed
    - “Prioritise ATC advisories”
BTC's Manoeuvring Decision (2)

- Observe (2):
  - carefully: there is one possible decision for BTC consistent with all their required procedures
    - with the exception of JAA Leaflet 11
  - and that is to descend
  - as we shall now see
  - and as BTC in fact did

BTC’s Manoeuvring Decision (3)

- Notice that BTC’s decision to descend is cited by the BFU as a causal factor in the accident

- It follows that
  - An appropriate manoeuvring decision was made by a participant in a TCAS interaction, given the participant’s rational cognitive state (RCS – see below)
  - This decision was causal in an accident

- I invite the conclusion that the sociotechnical system ACAS, which includes actors’ RCS’s as well as TCAS technology (see below, Issue 6), has been insufficiently causally analysed
Procedural Background

- ICAO PANS-OPS says nothing (including RAs) shall prevent PIC from exercising best judgement and full authority in avoiding a collision
- AIP Germany says follow an RA unless you have visually acquired the intruder and decided that no deviation from present flightpath is needed
  - but it also says never manoeuvre against an RA if it is decided not to follow it
- ICAO Rules of the Air say nothing, including RAs, can relieve PIC from taking action to best avoid collision
- LuftVO §13 Abs. 9 says that nothing, including requirements concerning RAs, releases PIC from the obligation to conduct flight so as to avoid collision

BTC’s Rational Cognitive State

- The Rational Cognitive State (RCS) of BTC CRW, the information state of the agent, is constructed from:
  (TCAS info) + (ATC info) + (other radio & cockpit info)
- BTC RCS included
  - a three-aircraft conflict
  - an advisory descent to avoid unpainted traffic
  - an RA ascent to avoid painted traffic
  - a clear night
  - painted traffic in sight
    - but lights only, no depth cues, no altitude cues
BTC's Decision Requirements

- Applicable decision requirements:
  - avoid collision as highest priority even over an RA manoeuvre
    (ICAO Rules of the Air, ICAO PANS-OPS, LuftVO §13 Abs. 9)
  - visual acquisition allows one not to follow the RA (AIP Deutschland)
  - main avoidance means: visuals and ATC advisories; secondary means: RAs (TU154M Ops Manual)

- Intuitively supporting but non-applicable requirements
  - BTC PIC shall initiate a descent (AIP Russia)
  - FAA AC120-55B similar to AIP Deutschland (above)

BTC's Rational Decision (1)

- Consider the following reasoning:
  - avoid the unseen target
    - one does not know where it is
    - ATC says descend
      - so it is either level or above
      - ascending might well exacerbate the conflict
  - avoid the painted target
    - one knows where it is (painted and visual)
    - RA says ascend (but contraindicated as above)
    - but one has visually acquired the painted target, so one may de-emphasise the RA
      - one may expect that descending will not exacerbate the conflict with the painted target
BTC's Rational Decision (2)

- Supporting reasoning from RCS
  - TU154M Ops Manual says prioritise ATC
- Supporting psychology
  - AIP Russia says descend on visual contact; one may presume this is a habit
  - Psychologically easier to avoid the aircraft you see than the aircraft you don't
  - Almost every procedure requires you to use your best judgement and authority above all

Consequences

- PIC discretion is enshrined in most aviation law
- Crew actions therefore depend essentially on RCS
- We have just seen: BTC crew RCS substantiates a discretionary manoeuvre in contra-sense to Eurocontrol advice and to BFU recommendation
- Note:
  - BTC crew RCS depends causally on one piece of (mis)information from ATC
Issue 6: What Components Has the ACAS System?

- ACAS avionics (AV): TCAS II V7 or V6.04a
- PF may not be PIC: resolving an RA needs CRW interaction
- For two-airplane situations there already 4-6 interacting system components: 2 AV + 2 CRW, each CRW with PIC & PF & PNF (two actors, three roles)
- But AV (2 components only of 6 minimum) is usually the focus of attention
- Many comments on ACAS rest on this equivocation between ACAS the system and TCAS the kit
What is the ACAS System? (2)

- ACAS avionics does not manoeuvre the airplane
- Therefore: ACAS System is at least: AV + CRW
- CRW behavior regulated by training and guidance materials (not uniform, indeed partly contradictory, according to BFU)
- Previous analysis shows this cannot suffice for satisfactory (dangerous-failure-free) system operation
  - There is presently no unique behavioral algorithm for ACAS
  - It could be that there is no universal constraint such as “never manoeuvre contrary to an RA” – see Issue 5

What is the ACAS System? (3)

- Issue 5 shows how ATC input causally affects (AV+CRW) and thus aircraft behavior with respect to ACAS:
  - ATC input causally affects CRW RCS
  - CRW RCS is part of (AV+CRW)-state
  - (AV+CRW)-state causally affects aircraft behavior

- Any input which causally affects system state or behavior must be analysed
- Note: Any input which may be controlled and which causally affects... is candidate to be part of system
Issue 7: ACAS System State

- Überlingen:
  - DHL RCS, BTC RCS, ATC RCS are all different from each other!
  - This difference is due to a cognitive mistake (of a well-known type) in one component

- Zürich ATC:
  +DHL posn, +BTC posn, -RA, -phantom AC
  (makes cognitive mistake 10/2 o’clock in advisory)
- DHL:
  +DHL posn, +BTC hrz posn, +RA +sense, -phantom AC
- BTC:
  +BTC posn, +DHL hrz posn, +RA +sense, +phantom AC
Conclusions Concerning These Issues

Specific Conclusions

1: ACAS Reversal-RA requirements are flawed.
2: ACAS-RVSM interactions must be more thoroughly analysed.
3: It must be determined where ACAS algorithms fail.
4: Advice on TCAS use must be uniform and unambiguous. Making it mandatory is inappropriate.
5: The operator RCS must be explicitly included in ACAS algorithm analysis.
6: It should be determined, by application of rigorous system reasoning, what components ACAS system has. That system should be causally analysed for weaknesses and failure.
7: This is the simplest sociotech system I know in which participants can so easily achieve mutually contradictory RCS’s. I know of no simple solution for this phenomenon.
Comments on Causal Reasoning

Causal Reasoning (1)

- The BTC CRW performed according to established procedures (confirmed by BFU) and manoeuvred consistently with a justifiable decision in a situation in which one can argue it was impossible for them not to break some rule

- The BFU singled out their manoeuvre, and that it broke a rule/system philosophy, as a causal factor

- BTC’s action was just as conformant with applicable procedure as DHL’s
Causal Reasoning (2)

- It follows that BTC and DHL as agents followed applicable procedure
- It could therefore be argued that the “nearest possible world” in which the accident did not happen was one in which ATC did not make his mistaken “2 o’clock” traffic call, but the correct “10 o’clock” call
- Call this factor the *most-variable causal factor (MVCF)*
  - Note: there may in general be many; MVCF is in general a set

Causal Reasoning (3)

- Thus Überlingen shows a situation in which the MVCF belongs to a system which many analysts argue should play no role!
- I see no way in which the ACAS system can be analysed without taking into account all causal influences on it, especially MVCFs of potential or actual incidents
- Nevertheless, some people still argue for ignoring ATC in ACAS analyses
Conclusion and Acknowledgements

General Conclusion

• Rigorous analysis of sociotech systems is in its infancy
• Despite this, much more can be done
  • E.g. formal verification techniques exist
• Safety problems with mechatronic systems pale in comparison with safety problems of sociotech systems in aviation
  • Accidents have been caused by failure of sociotech systems
  • Accidents have not been caused by failure of mechatronic systems (although often suspected)
• So let's pay sociotech systems more attention!
Acknowledgements

- Hardy Heinlin of Aerowinx for the TAU graphic
- Jim Kuchar of MIT Lincoln Labs for the multiple-aircraft pairwise-resolution counterexample and graphic
- Eurocontrol for diagrams from training materials
- BFU for the Überlingen collision graphics

The End

Thanks!