Causal Analysis of the ACAS/TCAS Sociotechnical System

Peter B. Ladkin

Faculty of Technology, University of Bielefeld, Germany
ladkin@rvs.uni-bielefeld.de
www.rvs.uni-bielefeld.de

Abstract. Sociotechnical systems are those which rely not only on technology but on humans and social organisation for their adequate functioning. The analysis of sociotechnical systems poses the particular challenge of synthesising methods appropriate to formerly separate scientific disciplines. One result is that prominent features of the systems are often missed during analysis. This paper points to some features of the ACAS/TCAS transport aircraft collision avoidance system which I believe could do with much closer scrutiny.

1 The Überlingen Midair Collision

Sociotechnical systems contain mechanical, electrical or electronic parts but rely for their appropriate functioning on human or social organisation and actions. Analysing them is often a complex matter, not only because the systems themselves are often complex, but because analysts must somehow apply a multitude of analysis techniques which traditionally have belonged to different scientific disciplines: computer science, physical and mechanical engineering, ergonomics, psychology and organisational theory.

On 1 July, 2002, a Tupolev 154M operated by Bakshirian Airlines (BTC), a Russian airline, was flying westwards at night over Southern Germany towards a destination in Catalunya. A Boeing 757 operated by the cargo airline DHL was flying northbound over Switzerland, at the same Flight Level 360 (representing a nominal altitude of 36,000 feet in a normed atmosphere). Both were operating under Instrument Flight Rules (IFR), compulsory at this Flight Level. Skyguide, the Swiss air traffic control organisation, had control of both aircraft, and accordingly responsibility for separation of the aircraft.

The controller on duty was operating two positions, some meters apart, because colleagues were on break. He was working primarily with other traffic at one position, and only noted the convergence of the two aircraft close to the point at which the separation he was required to enforce was to be broken (7 nautical miles lateral and/or 1,000 ft vertical separation). Another air traffic control facility at Karlsruhe had noticed the convergence, but was unable to contact Zürich through the dedicated communication channel, which was undergoing maintenance. Similarly, an automatic "early warning" system installed at the Zürich facility was undergoing maintenance and did not trigger.

The controller issued an avoidance manoeuvre to BTC to descend immediately. However, both aircraft received a Resolution Advisory from their on-board Airborne Collision Avoidance System (ACAS) devices, both TCAS II Version 7.0 from the company ACSS, virtually simultaneously with this instruction. TCAS advised to BTC an immediate climb, and to DHL an immediate descent (the manoeuvres expected are also normed: a smooth 1/4g acceleration to a climb, resp. descent rate of 1,500 feet per minute (fpm)).

DHL descended. The BTC commander also instructed his Pilot Flying (PF) to descend. 7 seconds later, the air traffic controller repeated his descend instruction to BTC with an note to "expedite", for traffic which he mistakenly described as at the "two o'clock" relative position. BTC was at "two o'clock" to DHL; DHL was at "ten o'clock" to BTC. Such cognitive slips are not uncommon, and normally not consequential. In this case, however, it caused the BTC commander to believe he was in a three-aircraft conflict, with DHL, whose lights the crew could see and had identified at their ten o'clock, and with an unknown aircraft which his TCAS display was not "painting", at his two o'clock [Bun04]. (I had speculated that this might have been so already in [Lad02a].)

7 seconds later, DHL received an "iterated advisory" to "increase descent" (to a normed rate of 2,500 fpm). 9 seconds after that, DHL informed air traffic control that he was in a "TCAS descent".

Air traffic control procedures are that they are no longer responsible for separating traffic responding to TCAS Resolution Advisories until it is reported to them by the participants that they are "Clear of Conflict". However, they may continue to provide information to participants during the manoeuvres. The air traffic controller conformed with this procedure.

11 seconds after DHL informed the controller of the TCAS descent, the two aircraft collided.

A more extensive discussion of the TCAS kit (the avionics that provides the information on nearby

Copyright (c) 2004, Australian Computer Society, Inc. This paper appeared at the *9th Australian Workshop on Safety Related Programmable Systems (SCS'04)*, Brisbane. Conferences in Research and Practice in Information Technology, Vol. 38, Tony Cant, Ed. Reproduction for academic, not-for-profit purposes permitted provided this text is included.

participating aircraft, as well as the manoeuvring advisories, to crew), as well as the precise minute-by-minute details of the accident, may be found in my presentation slides [Lad04] and the official accident report [Bun04].

Immediately after the accident, attention focused on BTC's descent contrary to his TCAS Resolution Advisory, as well as the various apparent procedural deficiencies at Skyguide. In a particularly sad and inappropriate incident, the controller involved, who was reported to be understandably personally very affected by what had happened, was murdered by what was presumed to be a distraught relative of an accident victim.

The responsible investigating authority, the German BFU, issued their final report in May 2004 [Bun04]. It contains a thorough discussion of the sociotechnical system consisting of the Skyguide air traffic control facility at Zürich, in my view an excellent example of this analytical art. Many factors contributing to the accident concern the operation of this system. In addition, BTC's decision to descend was cited as a factor. The TCAS avionics was found to have operated as designed and intended.

Also cited as a factor were the many, often contradictory, procedural instructions or advice to pilots on appropriate procedures on reception of a TCAS Resolution Advisory. The report enumerates all these pieces of advice and contains a thorough discussion.

The BFU recommends that it should be made mandatory for pilots to follow TCAS Resolution Advisories.

2 A Brief Description of the ACAS/TCAS System

First, some terminology. The name ACAS refers to an international standard, normed by the International Civil Aviation Organisation (ICAO), a subsidiary organisation of the United Nations. The specification comes from the U.S. TCAS system, developed over some thirty years, and mandated for commercial air transport in the U.S. by the U.S. Congress after a collision between an Aeromexico transport and a civil light aircraft in the Los Angeles area. I use the term TCAS here to refer to the avionics.

The TCAS avionics senses other similarly-equipped aircraft in its vicinity through use of the radar transponders with which all aircraft flying at these flight levels are equipped.

A transponder is a radio device which receives signals at the standard air traffic control radar frequency and automatically transmits information in return. So-called Mode C transponders transmit the aircraft ID, the aircraft's pressure altitude (an internationally-normed altitude which is a fixed function of the sensed outside air pressure, also used to define the Flight Levels), and a four-octal digit code, called a "squawk", which is set by the pilots during the flight according to air traffic control instructions. Mode S transponders, used by TCAS, have in addition to the Mode C functions also space in the return signal for sending a message.

The TCAS avionics uses Mode S for detecting other aircraft, for reckoning relative closing speed and altitude, and for negotiated avoidance manoeuvres (Resolution Advisories, RA) with the other close aircraft.

Whereas normal Mode S responds only to interrogation, in conjunction with TCAS avionics it broadcasts regularly "in the dark" as well as responding to broadcasts from other aircraft. The time lag or latency between a broadcast and receiving a reply is used to determine range (the distance to the responding aircraft). The latency is roughly composed of the time it takes the signal to traverse the distance between the aircraft, the processing latency of the receiving aircraft, and the time it takes the responding signal to return. The processing latency of the avionics is known (is normed as part of the kit), hence the range may be calculated. Altitude information comes directly from the Mode S altitude reports, which are discretised into (usually) 100 ft or 25 ft increments. Relative (horizontal and vertical) closing velocities are calculated from comparing successive returns.

Warnings (Traffic Advisories, TA) and RAs are issued based on a time period, called *Tau*, τ, obtained by dividing the range R by the closing speed dR/dt:

$$\tau \;=\; R\,/\,(-dR/dt)$$

The units of τ are seconds. The times at which TA and RA are triggered varies with altitude. Above Flight Level 200 (a pressure altitude of 20,000 ft), the typical times are 48 seconds for a TA and 35 seconds for an RA. This basic formula has been modified in recent releases of TCAS II, but the basic principle remains the same.

τ is primarily sensitive in the horizontal plane. Two aircraft converging to a point in the horizontal plane will not trigger warnings if they are sufficiently separated vertically. For example, under Reduced Vertical Separation Minima (RVSM), valid in European airspace between FL 290 and FL 420, aircraft may legitimately be separated by 1,000 ft altitude (that is, they may be cleared, one at, say FL 350 and one at FL 360, and cross paths). Previous, "conventional", separation at these levels was 2,000ft. For crossing aircraft maintaining constant altitude, a TA will be triggered by TCAS II V7.0 at 850 ft altitude separation, and an RA at 700 ft altitude separation, both less than the nominal 1,000 ft separation under RVSM. (There are some operational issues with use of TCAS II V6.4a, which issues TA and RA at larger separations, as well as the effects of turbulence and the normal feedback control-system oscillation of autopilot control. I consider these elsewhere [Lad02a].)

It is intended that a Traffic Advisory act as a warning to crew of another aircraft in the vicinity. A Resolution Advisory consists of an aural annunciation to “Climb, Climb” or “Descend, Descend” along with notification on the TCAS Graphical Display. A climb manoeuvre or descent manoeuvre is expected, with transition accomplished with a smooth accelaration of 1/4g to a climb/descent rate of 1,500 feet per minute. The RA may later be strengthened (e.g., “Increase Climb, Increase Climb”) by a so-called Iterated Advisory, whereupon a rate of climb/descent of 2,500 fpm is awaited. An RA may also be weakened, or even reversed (“Descend, Descend NOW”), depending on the subsequent behavior of the other aircraft (the “intruder” in TCAS parlance). TCAS II avoidance manoeuvres are expected strictly in the vertical plane only; course-altering manoeuvres are not foreseen or advised.

This brief synopsis has been based on the following sources. For operational details of ACAS, see [Eur00]. For detailed technical consideration of the criteria for TA and RA warning, see [FW04].

2.1 Some TCAS Philosophy

However, the avionics by itself just paints pictures on displays and makes audio announcements. Response to those displays and announcements is the responsibility of the crew of the respective aircraft. So the success of the collision avoidance system depends causally, essentially, on the crews using the TCAS information to manoeuvre. Thus the *avoidance* system includes the crews. I therefore use the term ACAS to refer to the entire avoidance system (whatever it might consist in - see Issue 6 below).

The discussion of TCAS philosophy owes much to discussions with Ed Williams of Airservices Australia [Wil04,Wil05].

TCAS is intended to be a system of last resort, that only triggers at the last possible moment at which a potential collision may be avoided. At that point, it is intended that unambiguous manoeuvring advisories will be issued by the TCAS system that, if followed, will avoid a collision between participating aircraft.

It is thereby thought to follow that the controller is “out of it”, and should be considered by crews responding to a TCAS Resolution advisory to be “out of it”, namely, the controller is thought to play no causal role in the TCAS choreography.

2.2 Some Issues With the ACAS/TCAS System

I enumerate below some issues which are not highlighted in the BFU report, but which I believe are important results of systems analysis. My main goal is to contribute to analysis of the ACAS/TCAS system. However, some findings cast considerable doubt on the BFU recommendation that TCAS Resolution Advisories be made mandatory. They also cast doubt on the “TCAS philosophy”.

Since BTC descended when TCAS advised “climb”, BTC’s actions came in for immediate comment after the accident, when it became apparent he had not been following what was presumed to be the “TCAS philosophy”.

3 Use of ACAS Played a Causal Role

First, there appears to be a common perception that, because the TCAS avionics functioned as designed, the “system” functioned as intended. It therefore seems appropriate to state the following theorem:

The use of ACAS played a direct causal role in the accident.

Proof:

- 1. DHL’s action to descend was performed by its commander following ACAS procedure after receipt of a TCAS Resolution Advisory
  (Justification: Report finding)
- 2. *Had* TCAS not issued the Resolution Advisory, DHL *would not have* descended (Justification: DHL’s clearance was for him to fly level at FL 360; there is no reason to suppose DHL’s commander would have deviated from clearance had he not received the TCAS Resolution Advisory)
- 3. *Had* DHL not descended, the two aircraft *would not have* collided (Justification: Calculations in the report show that the two aircraft collided some more than 600 feet below FL 360; some minor manoeuvring took place at the last moment. However, had DHL remained level at FL360, BTC would have passed some 600 feet or so underneath him.)
- 4. DHL’s descent formed part of ACAS procedures (Justification: By 2, using the Counterfactual Test, the TCAS RA was a necessary causal factor in DHL’s descent. Since ACAS procedures require a descent according to an RA in these circumstances, the TCAS RA along with following procedure form a necessary and sufficient set of causal factors for DHL’s descent. Since the commander’s following defined procedure is part of the ACAS system, as is the TCAS RA, it follows that the descent was exclusively part of defined ACAS system behavior, with no extraneous contributing factor.)
- 5. DHL’s descent was a necessary causal factor in the collision (Justification: Follows directly from Steps 2 and 3 using the Counterfactual Test
- 6: Conclusion. ACAS use was a necessary causal factor in the collision (Justification: Follows from Steps 4 and 5 by identifying DHL’s as solely part of ACAS procedure)
- QED.

The conclusion of this argument may be surprising. I invite those who may wish to contradict its conclusion, Step 6, to identify where it may fail.

No one has ever doubted the contentions in Steps 1, 2 and 4. Step 3 is a matter of fact. Step 5 is a matter of applying the Counterfactual Test, a test of necessary factorhood in causality used as part of the method WBA as well as by many investigators into causes.

So if you accept the Counterfactual Test, and you accept other contentions that everyone already accepts, you must accept the Conclusion.

4 The Issues

4.1 Issue 1: ACAS Requirements

TCAS has the capability to issue a Reversal RA some seconds after its initial RA, according to formal criteria that the continued movement of participating aircraft is not leading to the desired separation. An initial "climb, climb" RA will be followed by "descend, descend NOW" in a Reversal.

The aircraft were converging to a point at a relative speed of some 700 nautical miles per hour (knots, or kts. A nautical mile is about 1.15 statute miles, which in turn is about 1.6 km) [Bun04]. Furthermore, the aircraft were tracking each other more or less exactly in altitude all the way from FL 360 until collision.

I cannot imagine a more obvious criterion that the two aircraft remained continually on a collision path after the initial RA was issued. Yet the BFU says that the TCAS formal criteria for issuing a Reversal RA were not fulfilled [Bun04].

It follows that the TCAS formal criteria for determining if the aircraft remain on a collision path do not match all circumstances in which aircraft remain on a collision path, for example that the aircraft continue to track each other in altitude and converge to a point at 700 kts relative speed.

It follows from this observation that the formal requirements for determining if the aircraft remain on a collision path are faulty: they do not match their intention.

4.2 Issue 2: ACAS in the RVSM Environment

I have considered the issues of ACAS in the RVSM environment elsewhere [Lad02a,Lad02b,Lad03]. This issue did not directly arise in the Überlingen accident. However, the Überlingen accident casts doubt on some assumptions made in producing the Safety Case for RVSM procedures in European airspace [*op.cit.*]. See also [Lad04] for a summary of some of these issues.

4.3 Issue 3: ACAS Algorithm Correctness

The ACAS algorithms have been formally proved correct for two-aircraft interactions [LLL00,LLL99]. It has also been observed that pairwise-resolution algorithms such as those used with TCAS kit cannot resolve certain multiple-aircraft configurations [KY00,KY97]. However, one might wish to argue that the multiple-aircraft-configuration counterexample displayed by Lee and Kuchar might be rare enough to ignore in practice. Since we know, though, that ACAS algorithms, being pairwise-resolution, will fail to resolve some conflicts (no matter how rare they may be), the question arises: what is the minimal number of aircraft, and in what configuration, for which the ACAS resolution algorithms fail?

In 2002 I considered a number of three-aircraft configurations [Lad02a]. Most of them were resolved satisfactorily under iterated pairwise resolution, given the specification that TCAS is able to resolve pairwise relative speed differences of up to 1,200 kts closure rate and 10,000 fpm vertical closure rate [Eur00]. However, one configuration remained undecided by applying the pairwise-resolution logic. To date, it is unknown whether this configuration is indeed resoluble in ACAS logic, or whether there is an example of this configuration which allows a collision between aircraft A and C.

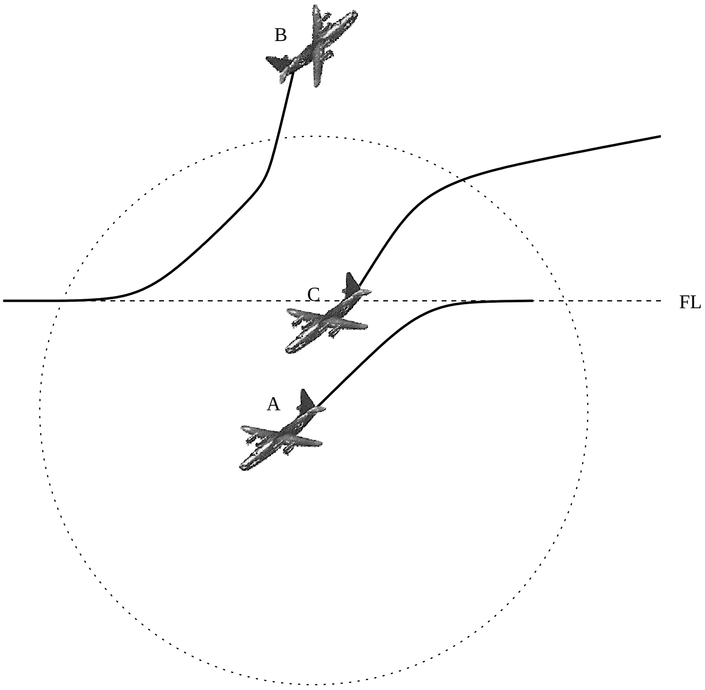

Fig. 1. An Unresolved Conflict?

In Figure 1, Aircraft A and B have been flying towards each other, whereas Aircraft C is descending towards them. There is a race condition; one of the conflicts must be resolved first. Let it be A-B, whereupon B receives a climb RA and A a descend

RA. The B-C conflict must then be resolved, with an increase-climb RA to B and a descend RA to C. C is, however, already inside the "protected zone" of C. How is the A-C conflict resolved?

The correctness of ACAS algorithms is known for two-aircraft conflicts. It appears not yet to be known for all three-aircraft conflicts. Nevetheless, the BFU recommended that adherence to ACAS procedures be made *mandatory* upon commanders. Not only would this be an unprecedented step in the history of aviation, during which until now the final decision responsibility for the safety of the aircraft lies with its commander, including during ACAS encounters, but it would be remarkable in that algorithms and manoeuvres would be mandated that are not yet known to be formally correct.

4.4 Issue 4: Conflicting Advice on TCAS Use

The BFU report assembles all the relevant procedural information. The most salient are these:

Eurocontrol literature advises pilots always to follow an RA

ICAO Annex 2 Ch. 3, 3.2.2 position is that nothing relieves a pilot in command (PIC, the aircraft commander) of responsibility for 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 TCAS TAs and RAs) shall prevent PICs from exercising their best judgement and full authority in the choice of a course of action to resolve a traffic conflict

The European Joint Aviation Authority (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. The distinction between "should" and "shall" is important, as follows.

UK CAA clarifies their use of the word "should" rather than "shall": "...to allow for Commanders'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".

Luftfahrthandbuch 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

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

The Tupolev 154M 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 crew, 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

All these applied to the Überlingen situation, with the exception of the UK CAA pronouncement. ICAO PANS-OPS and the other documentation is intended to provide guidance everywhere; the participating aircraft were in German airspace and thus the LuftVO was in force and the Luftfahrthandbuch provides guidance; this airspace is within that for which Eurocontrol intends its advice to hold; it is also within the JAA regulations domain of application. Further, the Tupolev 154M Ops Manual governs procedures on board the TU154M of BTC.

Relevant guidance may also be found in

FAA Advisory Circular 120-55B dated 22.10.2001 says that the Pilot Flying should manoeuvre as indicated by an RA unless doing so would jeopardise the safe operation of the flight, or the crew can assure separation through definitive visual acquisition of the intruder

It should be obvious that, for example, the Tupolev Ops Manual contradicts JAA Leaflet 11, and the Eurocontrol advice always to follow an RA conflicts not only with the Tupolev Ops Manual but also with the UK CAA advice and the Luftfahrthandbuch Deutschland, as well as the FAA Advisory Circular.

Apart from these contradictions and conflicts noted by the BFU, the general tone of most advice, except for that of Eurocontrol and the Tupolev Ops Manual, is to follow an RA unless the Commander has good reason not to do so.

So did the BTC Commander have a reason not to follow the RA?

4.5 Issue 5: Operator Cognitive State and the Decision to Descend

Consider the cognitive state of an ideal Commander in the BTC cockpit. I am not concerned here with psychological aspects of a decision, or even with the actual way that (we might believe, or speculate, that) a decision was made in the incident, but instead with the reasoning available to an ideal reasoning agent in the Commander's situation.

Looked at crudely, *there is no possible decision for BTC consistent with all their required procedures*

Proof:

- 1: “Follow the RA” (Eurocontrol, and thereby Russian training; also JAA Leaflet 11 says to follow the RA in case of conflict with ATC advice)
- 2: “Need not follow the RA, but don’t go against it” (AIP Germany says not to manoeuvre against; and you may not follow an RA if you have visually acquired the intruder, which BTC had, and decided that no deviation was needed)
- 3: “Prioritise ATC Advisories” (Tu 154M Ops Manual)

Since ATC said descend and TCAS said climb, it is clear that these applicable advice and regulations are contradictory.

In this case, any decision that the Commander made would contravene some applicable regulation as it is stated above, without the caveats. Include the caveats, however, and it turns out that there is one decision available to BTC which is consistent with all their required procedures, *and that is to descend*.

I describe first of all the notion of *Rational Cognitive State* (RCS). The RCS of an agent is that information about the state of a system which the agent has received, or which the agent may (correctly) infer from the state information received.

The RCS distinguishes itself from the physiopsychological state of a human agent in various ways. One way is that there are no cognitive restrictions on the RCS. For example, it is known that humans in general are able to distinguish four to six warning sounds fairly well, but ability to discriminate sounds falls off rapidly with the addition of more aural warnings to these [Pat90]. Consider a situation in which 12 auditory warnings sound at the same time in a cockpit. The RCS of a pilot would include the information “Warnings A1, A2, ... A12 are sounding,” whereas any human pilot would only be able to conclude “Some number of warnings are sounding” through the psychophysiological restriction on hisher auditory perception. Another way is because of a human’s individual characteristics. For example, a pilot may forget state information, or even not perceive it or not assimilate it when presented. In these ways and others, the RCS is not necessarily a good model of a pilot’s likely cognitive state. However, it contains the largest possible superset of the cognitive state information: any state information it is possible for the pilot to have obtained is in the RCS.

In the case of the Überlingen encounter, the RCS of the BTC commander was constructed from TCAS info + ATC info + other info inferrable from radio communications and from cockpit displays. BTC’s RCS included

- a three-aircraft conflict
- an advisory descent to avoid unpainted traffic
- a TCAS resolution advisory ascent to avoid painted traffic
- a clear night
- painted traffic in sight
    - but lights only, no depth cues, no altitude cues

The applicable requirements for BTC commander’s decision were

- avoid collision as highest priority, even over an RA manoeuvre (ICAO Rules of the Air, ICAO PANS-OPS, LuftVO)
- visual acquisition of the TCAS “intruder” allows one not to follow the RA (Luftfahrthandbuch Deutschland)
- main means of avoidance are visuals and ATC advisories. An RA is a secondary means (Tu 154M Ops Man)

Consider the following decision reasoning:

- avoid the unseen target
    - one does not know where it is
    - ATC apparently does, and instructs to descend
        - so it is either at FL 360 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
    - visual acquisition, so one may deemphasise the RA
    - with visual acquisition, descending may not exacerbate the conflict as strongly as it would without visual contact

This indicates a descent towards a target which is both displayed and visually acquired might be preferable over an ascent towards a target which one does not paint and which has not been visually acquired. Psychological support for such a decision may be gleaned from the considerations.

- It is easier to believe that you can avoid an aircraft you see more easily that an aircraft you don’t see, so if you have to manoeuvre towards one, it is easier towards the one you see
- AIP Russia says descend on visual contact. Although not applicable in German airspace, one may presume this is a habit
- almost every procedure requires a commander to use hisher best judgement, assimilating all information

PIC discretion is enshrined in most aviation law. Crew actions in response to TCAS RAs, indeed to any situation, depend essentially on the RCS. We have just seen that BTC’s RCS substantiates appropriate decision-theoretic reasoning to a manoeuvre *in the contrary sense to the RA*, which is contrary both to Eurocontrol advice, *and to the BFU recommendation to make RA-following mandatory*.

Note that the BTC RCS depends causally on one piece of (mis)information from air traffic control, namely that there is a conflict with traffic at

BTC's two o'clock position. This traffic did not exist - this was a cognitive slip - but it was present in BTC's RCS.

To reiterate: this decision-theoretic analysis is just that: theory. I do not suggest in any way that this is the way BTC indeed reasoned. What is important is that, given the misinformation from air traffic control, and BTC's RCS, causally dependent on that information, there is appropriate decision-theoretic reasoning leading to a descent manoeuvre.

However, this is not a one-off case. The decision problem is real. It arises in a simultaneous conflict with a threat whom one does not paint or see, but whom ATC sees, and a TCAS "intruder" whom one both paints and sees, and in which the TCAS RA advises to manoeuvre into the airspace occupied by the unseen threat: Here is the decision problem presented to a rational pilot:

- You receive an ATC instruction to descend for traffic.
    - Therefore you infer that the "threat" is at your flight level or above
    - You do not have visual contact with the threat
    - *Therefore* the airspace at your Flight Level and above is not available for you to manoeuvre
- Simultaneously, you receive a TCAS Resolution Advisory which advises you to climb
    - You have visual contact with the "intruder" painted by TCAS
    - The airspace above you is closed for manoeuvring because of the presence of an unseen threat
- What do you do?

To summarise:

- There is a causal path in the ACAS system, from an input representative of a common cognitive slip, through appropriate decision-theoretic procedures, to a participant manoeuvring contrary to an RA in a two-aircraft TCAS encounter
- There is a three-aircraft TCAS decision problem which is not satisfactorily resolved by the common procedural advice always to follow the RA.

This phenomenon is, or should be, considered as a problem for ACAS. Especially since the BFU recommended making the following of RAs mandatory.

4.6 What Are the Components of ACAS?

All agree that the TCAS II kit is a component of the ACAS system. However, as I have pointed out, the kit by itself *does not* manoeuvre the aircraft for collision avoidance. The crew of each aircraft must undertake that manoeuvre. It follows that the crew of each aircraft are a functionally necessary part of the Airborne Collision Avoidance System. Without a manoeuvre, there is no collision avoidance, no matter what the TCAS II kit is showing or saying.

The crew itself might be further decomposable as a system. Suppose that the Pilot Flying (PF) is not the Pilot in Command (PIC). The responsibility for the decision on the manoeuvre lies with the PIC, but the crew member who must carry it out is the PF, and these may be two different people (as was the case for BTC in the Überlingen accident, although not for DHL). If PIC and PF are different people, communication and coordination is required between them to decide on and execute the manoeuvre.

It follows that even in a two-airplane ACAS encounter, there are between four and six major interacting components (two TCAS II kit installations and two PFs, and maybe PICs if the PIC is not PF at the time).

However, there were many comments after the Überlingen accident that "the TCAS system" performed perfectly. Such comments give rise to an equivocation, which was exploited by some. The equivocation is resolved as follows: the TCAS II kit performed perfectly; the ACAS system, which incorporates the crews also, arguably did not. The BFU itself was careful to distinguish the TCAS kit from the other components of the system.

So far, we have that

- Since the avionics kit does not manoeuvre the airplanes, the crews do, and such a manoeuvre is a function of the system, the crews are a component of the ACAS system
    - Let AV1 and AV2 be the two TCAS kit, CRW1 and CRW2 the two crew, $\supseteq$ the containment relation for systems and their components, and + the composition operation for system components. Then:
    - ACAS $\supseteq$ AV1+AV2+CRW1+CRW2
- Since the PF manoeuvres the airplane, and the decision to and how to manoeuvre rests with the PIC, both are – either distinct or identical – components of CRW
    - CRW $\supseteq$ PF+PIC

Furthermore, Issue 5 has shown that input from ATC causally affected the BTC RCS, and the RCS is part of the state of the BTC crew. So we have that

- ATC information causally affects CRW RCS
- CRW RCS is part of CRW state and therefore of ACAS system state since ACAS $\supseteq$ AV1+AV2+CRW1+CRW2
- CRW-state causally affects aircraft behavior through RCS input to decisions, as discussed earlier

Any input source which causally affects system state or behavior must be analysed. Note that this input source *alone* allows a decision by BTC that was crucial to the outcome of the encounter, as I have just shown. The question could be raised whether air traffic control, contrary to the TCAS "Philosophy", is thereby best considered to be part of the ACAS system. I suggest that this question, primarily one of delineation of the system boundary, is less pressing than that of ensuring that system behavior under all causally-significant inputs are adequately analysed.

Note that there is a discrepancy in RCS between the time at which an RA is announced (simultaneously to both crew) and the time at which one crew informs ATC that they are performing a TCAS manoeuvre. This was particularly long in the case of Überlingen, for reasons explained in the report: some 23 seconds. During these 23 seconds, ATC issued its iterated descent advisory to BTC which including the erroneous information of the traffic at two o'clock.

It follows that an actor whose informative role we have shown to be causally significant (ATC) has, for some crucial seconds at the beginning of a TCAS manoeuvre, an incorrect understanding of some of the state of the system (heshe is unaware of the presence of a TCAS RA until it is announced to himher). One can consider this to be anomalous, especially in light of the role change required of this actor (to relinquish responsibility for separation and to restrict communication to informational communication only). ATC is still capable of causally-significant input during such a manoeuvre, and since such input may be based on a false view of system state, I believe this situation should be more thoroughly analysed than it has been to date.

4.7 Mutually Contradictory Partial System States

In the Überlingen accident, the three causally-relevant actors, ATC, DHL CRW and BTC CRW, had mutually contradictory understandings of the system state for significant parts of the incident. I use the following acronyms:

- posn: vertical and horizontal position
- hrzpn: horizontal position
- alt: altitude (vertical position)
- RA: an RA has been issued
- sense: the sense of the RA is known
- phantom: there is a (third) aircraft at BTC's two o'clock

I indicate who has what information, and who has it not, with + and - signs.

Here are the RCSs of the three main actors during the crucial initial few seconds of the encounter.

ATC +DHL posn, +BTC posn, -RA, -phantom

DHL CRW +DHL posn, +BTC hrzpn, -BTC alt, +RA, +sense, -phantom

BTC CRW +BTC posn, +DHL hrzpn, -DHL alt, +RA, +sense, +phantom

Thus ATC did not know of the RA; both others did. BTC "knew" of the phantom; both others did not. DHL knew both of the RA and no-phantom; both others knew one or the other but not both.

This is the simplest example I know in which a small number of system agents can obtain three mutually contradictory ideas of the system state through a single input – and that input, although a slip, is a common type of slip.

5 Conclusions

To summarise the issues which have been raised:

- Use of ACAS was a necessary causal factor in the collision
  1. The aircraft continued to converge at 700 kts while tracking each other in altitude, after issuance of the first RA. However, the technical requirements for a Reversal RA were not fulfilled. Thus the technical requirements for Reversal RA do not match all conditions under which one should be issued. This is a requirements mismatch.
  2. There are issues with ACAS use in the RVSM environment (not considered here).
  3. ACAS algorithm correctness is known for two-aircraft interactions. It is not known even for three-aircraft interactions. It is known to fail for some multi-aircraft configurations.
  4. As noted by the BFU, applicable procedural requirements and guidance on ACAS use are mutually contradictory and otherwise non-uniform.
  5. A decision-theoretic analysis based on participants' RCS shows that a participant could decide, in certain circumstances, to manoeuvre against an RA, using appropriate decision procedure. However, such a manoeuvre is procedurally proscribed.
  6. The components of ACAS include at least two sets of avionics and two sets of crew. Further, a crew consists of PF and PIC, and these may not be the same person, requiring interaction between them in the case of an RA. Since the actions of at least one component (the BTC crew) were identified as a causal factor of the accident, it cannot be correct under this view to claim that "ACAS functioned as designed in this accident." It most certainly didn't: one component acted contrary to design. Further, a causally-relevant actor, namely ATC, has for a period of time at the beginning of a TCAS manoeuvre necessarily a false view of the system state.
  7. The three causally-relevant participants in the Überlingen accident had, for a signification proportion of the ACAS interaction, three mutually contradictory understandings of the system state. Indeed, ATC's

unawareness that an RA had been issued allowed him to issue one causal input which can lead through appropriate decision procedures to a participant manoeuvring contrary to design.

What follows from these? Here are my opinions.

1. The TCAS criteria for issuing a Reversal RA should be reworked to subsume all cases in which a Reversal is needed, such as continued high closing speed and continued identical or closely-similar altitude.
2. The interactions between ACAS and RVSM should be more thoroughly analysed than they so far have been.
3. It should be precisely determined in which circumstances ACAS algorithms are correct and in which circumstances they fail. In advance of such knowledge, suggestions to mandate following an RA for pilots are at best premature and at worst potentially dangerous.
4. Requirements and advice on ACAS procedures for pilots should be deconflicted. If not worldwide (because of insuperable administrative problems) then at least locally, so that every pair of interacting crews has a common understanding.
5. Interactions in the ACAS system should be causally analysed using (at least) participants' RCS and decision theory.
6. The causal consequences of necessitating a false view of system state for one causally-relevant actor should be thoroughly investigated, for few distributed-system algorithms exist which allow this phenomenon. Another option is to avoid this phenomenon: enunciation of RA issuance to ATC can be automated.

6 Final Comment

ACAS is a hybrid system in the sense of informatics, in that it has not only components and behavior which can be analysing using discrete-system techniques (such as developed for finite-state systems) but behavior which involves continuous mathematics (that of dynamics). Although the system has been in development for some thirty years, essential parts of the casual analysis, especially those involving phenomena conflicting with the "TCAS philosophy", seem not yet to have been performed. Let us start to do so.

References

[BBR90] D. E. Broadbent, A. D. Baddeley, and J. Reason. *Human Factors in Hazardous Situations.* Clarendon Press, Oxford, 1990.

[Bun04] Bundesstelle für Flugunfalluntersuchung. Investigation report: Collision between boeing b757-200 and tupolev tu154m, near überlingen, lake constance, 1 july 2002. Technical report, Bundesstelle für Flugunfalluntersuchung, May 2004. Accessed on 12 Jan 2005 at `www.bfu-web.de/berichte/index.htm`.

[Eur00] Eurocontrol. ACAS II (Training Brochure). Document ACASA/WP6.1/015 of the ACASA Project, May 2000. Accessed on 12 Jan 2005 at `www.nbaa.org/intl/acas.htm`.

[FW04] N. L. Fulton and M. Westcott. A review of vertical proximity specifications of the Traffic Alert and Collision Avoidance System (TCAS). Technical Report CMIS 2004/167, Commonwealth Scientific and Industrial Research Organisation (CSIRO), Canberra, Australia, 2004.

[KY97] J. K. Kuchar and L. C. Yang. A survey of conflict detection and resolution modelling methods. In *Proceedings of the AIAA Guidance, Navigation and Control Conference*, number AIAA-97-3732, 11–13 August 1997. New Orleans, Louisiana.

[KY00] J. K. Kuchar and L. C. Yang. A review of conflict detection and resolution modelling methods. *IEEE Transactions on Intelligent Transportation Systems*, 1(4), 2000.

[Lad02a] P. B. Ladkin. ACAS and the South German Midair. Technical Report RVS-Occ-02-02, RVS Group, University of Bielefeld, August 2002. Available from `www.rvs.uni-bielefeld.de` → Publications.

[Lad02b] P. B. Ladkin. The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed. Technical Report RVS-Occ-02-03, RVS Group, University of Bielefeld, August 2002. Available from `www.rvs.uni-bielefeld.de` → Publications.

[Lad03] P. B. Ladkin. The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed. Update on WWW-site of RVS Group, University of Bielefeld, 2003. Available from `www.rvs.uni-bielefeld.de` → Publications.

[Lad04] P. B. Ladkin. The Causal Analysis of Sociotechnical Systems I: The Collision Avoidance System ACAS/TCAS. Available on 12 Jan 2005 from `www.rvs.uni-bielefeld.de` → Publications → Lecture Notes, January 2004.

[LLL99] C. Livadas, J. Lygeros, and N. Lynch. High-level modelling and analysis of tcas. In *Proceedings of the 20th IEEE Real-Time Systems Symposium*, pages 115–125, Phoenix, Arizona, December 1999.

[LLL00] C. Livadas, J. Lygeros, and N. Lynch. High-level modelling and analysis of tcas. *Proceedings of the IEEE*, 88(7), July 2000.

[Pat90] R. D. Patterson. Auditory warning sounds in the work environment. *Phil. Trans. Royal Soc. London B*, 327:482–492, 1990. Appeared in the volume [BBR90].

[Wil04] E. Williams. personal communication. Brisbane, Australia, 19–20 August 2004.

[Wil05] E. Williams. The airborne collision avoidance system. In Tony Cant, editor, *Proceedings of the 9th Australian Workshop on Safety-Critical Systems and Software, Brisbane, 2004*, volume This volume of *Conferences in Research and Practice in Information Technology*, Sydney, Australia, 2005. Australian Computer Society. Available from crpit.com.