Transcript of interview with ATC

R: Interviewer

M: Air traffic controller

R: So firstly, before we look at the models could you say a little about your experience and your work in air traffic control?

M: OK, so my role is what is called area controller: I deal with aircraft in flight through controlled airspace, a controlled volume of airspace where certain interactions happen with flights, so basically deconfliction and expeditious flow of traffic.

R: OK, so can I ask how long you've been in this field.

M: It will be soon ten years.

R: So have you been in this area controller role throughout your time or have you been in other areas?

M: No, you tend to train on specific sectors and generally achieve a minimum of validation and generally continue with those indefinitely.

R: Could you say a little bit about the area of airspace you cover?

M: So generally in air traffic apart from; you have aerodrome, approach and area functions. Within area you have upper airspace and lower airspace, in part because of the different performance of aircraft at different heights. So the job I do is the lower airspace, up to about 25000 feet or thereabout and it just means that aircraft perform in a certain way and generally say in the case of jets they'll be descending or climbing, but we have props or turboprops that will be cruising at those sort of levels. That's pretty much the area I work in.

R: So you don't cover jets at cruise, and you don't cover takeoffs and landings either?

M: Yeah, that's fairly accurate. Jets tend to cruise at anything like 30,000, 40,000 feet, so at the levels I work at they would mostly be in the climb or descending.

<Introducing the model>

<Stopped transcription at 0:02:30>

<Resumed at 0:12:16>

R: So what we have is a large model, essentially of air traffic pilot interaction around an event where a TCAS event has been generated and shown to the pilot. What we do first of all, because it's such a large model is to look at certain subsections, separately and then look at the whole thing put together.

R: We shall look at the first sub-set, some of the interactions around air traffic control. So you can see the interactions of several actors involved… Just have a look at that for a moment.

[about 30 secs passes]

M: I take it PF, that's pilot flying

R: Yes, that's our abbreviation for pilot flying.

[R gestures to ANSP actor]

R: That's our air navigation service provider.

M: So just a couple of immediate things: pilot flying, that's a term for the pilot who is flying the plane at the time, but obviously there are two pilots, so it could well be that the pilot that informs a TCAS RA could be the pilot not flying, I'm not sure…

R: [Interjecting] So we have the pilot not flying modelled for a couple of things which you'll see at the full model, but it's a fair point – I think based on what we have read that the regulations specify that the pilot flying was the one specified, required to inform…

M: But you might be right,…

R: I think at this point we can turn on, yes, these annotations that tell us where certain parts were found; so we mainly constructed this by looking the ICAO manuals for ACAS, and this tells us where the elements came from.

R: Now firstly, can I ask you if you could sort of talk us through, describe to us what representation of the system this model gives; sort of describe the model for us first of all, how you interpret it?

M: I still have a couple of questions, so um: TCAS here [referencing the TCAS actor], is the actual equipment on the aircraft?

R: Yes

M: So why is it pointing at this [the Report RA responsibility]

R: So a subtlety of the model notation there – it's greyed out slightly and the line is dotted; this based on the fact that we read in the ACAS manual there is in theory at least this provision for a system where the TCAS can automatically report alerts generated down to ATC; as I understand it that has never been implemented.

M: I haven't heard of it, no.

R: Apparently, in theory we are told this exists as a capability that is written into the standards as we understand it, based on the lines of we should do this following some detailed implementation that will be described somewhere else, and no-one ever described it. It would be relevant if it was in use.

M: One of my first questions – this model is trying to represent what is happening when a TCAS event happens

R: Yes, basically in the very immediate run up to the event, as it happens and then when it is resolved, rather than being a model of air traffic control, aircraft in general.

[time passes – about one minute]

M: Another is that, you know a pilot receiving an RA is expected to execute the manoeuvre straight away -

R: Yes, we have some more details on that in another part of the model.

M: So this is more to do with the air traffic controllers…

R: Basically in this sub-section we are limited to the interactions directly involving the air traffic controller, and some of the actors you see here have their own interaction that are going on at the same time but we aren't showing for reasoning of simplicity, but you'll see them later. This is basically all the interactions that air traffic control would be directly involved with.

R: So, could you I ask you a couple of questions about it. So can you broadly follow the structure of the model; for example, can you see how the parts relate to each other; what elements rely on other elements and so on; is that relatively clear or do you find it hard to follow?

M: Well a bit yeah, so I'm guessing you run through several options of what it could be, like, one of the responsibilities is for the pilot to inform the air traffic when they've had an RA; you have an alternative scenario where maybe an instruction has been given and they're unable to comply and the other one is when the resolution is issued you have to crosscheck to see if it's contrary to the RA, what the RA is saying.

R: These are things they may have to do; they don't have to physically do each of them simultaneously.

M: Just to recap on the arrows the solid black arrow is they are responsible for that, but the empty one is that they're also accountable for that -

R: Yes, yes – the solid arrow is that they are required to perform some action in response to this, the hollow arrow is that in some form they will be held accountable. So I think in this one there, basically [selects relations between PF and "Inform ATC..."]; there aren't many examples of one but not the other, but there is one there, I think.

Yes – the air traffic controller has to address the conflict if some conflict is occurring, a sort of abstract duty and to do that they need the co-operation of the pilots; what we've modelled here and you can tell me if this seems a reasonable description of the scenario that if there is a conflict occurrence then the primary responsibility and blame, if you want, would go to the air traffic controllers. Is that?

M: Could you expand on the scenario, so you're saying the pilot's complying with an RA but he gets into confliction with someone else -

R: I was thinking of the lines where you as an air traffic controller see some potential conflict about to occur and you say, your response is to issue an instruction to some pilot, some aircraft and the pilot for whatever reason does not respond, does not follow – then in that case, then if some failure of separation occurred as a result of that, would the sort of blame be placed on the controller for it happening or would the air traffic controller be allowed to say, well I issued this instruction to this pilot and they didn't follow, so it's that pilot's fault.

M: I think that might be an oversimplification, like in this case they wouldn't exactly be looking at blame, they'd be looking at maybe causality in a way; there wouldn't exactly be an allocation of blame so, you know, more like a Catch-22 scenario. You really couldn't just say it's the pilot's fault or it's the controllers fault, so I'm not exactly sure in that scenario; I can't see it being a blame, even

though another thing I would point out is with safety investigations it's supposed to be a blame-free culture or you know, not just looking at someone who's accountable and might be at fault, but looking at understanding what's happened and the mechanism to prevent that happen in future. So in that sort of event I don't think you could hold any one person accountable if anything the whole system -

R: A systematic failure?

M: Yeah, something like that, so…

Yeah, I'm trying to imagine an example, but clearly an aircraft following an RA is no longer under the control of the controller, so if it was in conflict with some other aircraft then the controller will immediately turn to the other aircraft which are still under his control to try and establish some form of separation; and then another thing you do in this sort of scenario where a RA puts your aircraft in conflict – it's OK that I don't have control of him but I can't still provide him with information saying OK, he might say "TCAS Climb" for example and I can say "You have traffic here at such and such" because one thing I mentioned is that the TCAS parameters for separation are completely different from the separation standards we use, so clearly TCAS might say that other aircraft is not in conflict because there is no risk of collision, but from our separation standards it is a loss of separation, so you try to avoid that too.

R: Your standards are stricter than those of the TCAS system?

M: Well yes they're essentially just bigger gaps and you know in that case you are saying I give you this traffic information, I mean generally TCAS is limited to a vertical profile but you don't exactly, the pilot might be flying manually and pull and turn the aircraft as well or you know, just to keep the picture.

R: So you're almost sort of, almost as they are responding to the alert you are also providing them with information to try and get a better result. So they might sort of..

M: Yes, or at least preventing a worsening situation. I mean, I'll give you an extreme example – the hold. So in the hold you might have ten aircraft flying on top of each other, in circles, so basically, vertical separation is the mode of separation we have – you know 1000 feet, barely 300 metres. So if you think you have ten aircraft stacked and then say the top one, for whatever reason descends either too sharply or busts a level, goes through the cleared level that you gave it and triggers an RA – you can imagine the domino going, and I believe this has happened before – not to me! But I believe this happened before, so it triggers a whole set of RAs, so you suddenly have ten aircraft trying to avoid, so in theory most likely outcome is they all end descending a little bit. So what you would do is pass traffic information – OK, you've got an RA for descending, but you're in the hold, there are five aircraft below you for example; you'll be almost like some limitation, some damage limitation -

R: So you're telling them like – yes, descend, but don't descend too much?

M: Well, not quite – it's almost like because in that scenario they are all going in circles, you can imagine that you know they can be literally converging, and because they're going in a circle they're descending, the whole pattern is very chaotic so they can get very very close and not just with one aircraft but potentially in that scenario with five or six – so you're saying "well, there are

five aircraft below you", for example, so the pilot as well as complying with the RA they might also be looking out the window even or looking at their FMS to see; it's about situational awareness I would say; OK, you're complying with this one RA, one instruction but there are implications beyond that you might want to consider as well. I would say that's kind of maybe -

R: That's a very interesting behaviour that we didn't really get out of reading the documents; what we've got, what we've modelled here is that they get their RA, they keep following that; basically, you get the RA and at that point you ignore the air traffic control until the RA computer tells you its resolved and then you speak to air traffic control again. You're saying that while you are following this process you are still getting information from the controllers and you're trying to use that to minimise the disruption, in effect.

M: Yes, or at least to prevent the situation from worsening, because like I say in that example with the holding, the situation can very quickly escalate, so while you not supposed to give any instruction you're providing a bit of information that might give a bit of context to where that aircraft is and what it potentially might…

R: I see – so it's not, you're not formally giving them instructions but just saying be alert, be aware of this?

M: Exactly.

R: And that might cause them to change their route slightly, based on…

M: Yeah, it might modify their behaviour slightly, so for example a TCAS RA generally, it is a vertical instruction to climb or descend and it gives you a range, you might have seen this, a range of compliance so you need to stay within this range to miss that other aircraft so it might be say climb between two and three thousands feet a minute or whatever, so if you stay within that range you miss; so if I've told the pilot there are five aircraft below he might stay in the lower end of that RA – does that make sense?

R: Yes, so he'll continue to follow it but take the sort of lowest acceptable difference -

M: Yeah, for example, or maybe he'll look at that point where the RA has been completed, and then start quickly level off, or even adapt, continue with the profile but actually start turning away from some aircraft you've told them is on the other side, so like I say it's about trying to maintain the situational awareness and do so while still being hands off; I don't have the control here but just so you know this might be…

R: That's a very interesting subtlety that we had not picked up on from looking at the regulations themselves -

M: Yeah, the manuals they try to stay quite clear and simplistic, black-and-white -

R: That's one of the things we're particularly interested in, is the by-the-book regulations, what the documents and instructions tell you is often not an accurate representation of how people do many tasks.

M: Absolutely, yeah.

R: And in many ways that's a strength, like in this case where the behaviour is off-specification, off

the exact defined process but gives advantages in this case by reducing the effects on the traffic.

M: I will give you another example, which I think is the same; one that I had is two aircraft that were cleared to if you like, safe levels but because of the climb rate and the descend rate one of the aircraft got an RA, so he did exactly by the book – RA, climbing so he bounced off the level and then went back; so, my response there was Roger – you acknowledge it and don't give any further instruction, but I did say "Yeah, the traffic, you have traffic here which is cleared one thousand below your cleared level" if that makes sense, so I'm kind of saying Yes, I think the RA has been triggered by this aircraft which is also under my control and which has been given a safe clearance, so it's a way of saying well, it something that; I'm not implying that it be a spurious alert, but it's kind of saying it's not something I've just pointed them at.

R: So you sort of saying - to me it seems to be safe, as far as I can see -

M: Yes, so the clearances were safe but for whatever reason, the aircraft performance or something has triggered this, so it's a way of saying, well this wasn't supposed to happen.

R: That's sort of like saying to them, take a slightly more gradual approach perhaps, or less aggressive manoeuvres than if so; I see this [garbled]

M: Possibly, yes. I think it is also, with this extreme case there's also that sort of emotional response; you really make like brisk [garbled] and you know it's a way of saying, I don't know how to say but sort of take some of the initial fear reaction from the situation – does that make sense?

R: Yes, OK.

R: So, is there anything in this model, other than what you've already said that seems to be inaccurate that you wouldn't recognise as.. -

M: I was going to mention about the STCA – so STCA is radar based essentially, they don't always trigger in an RA event and the same thing, it has different parameters for triggering; so I'm saying that in any TCAS event you don't necessarily have an STCA alert, so..

R: Would we say that, do they ever overlap, are there cases?

M: Well, yes; I'll give you another example. STCA has, I'm not entirely sure of the parameters; say a general standard of separation is one thousand feet vertically, five miles laterally so STCA maybe said at four miles laterally and eight hundred feet vertically so if it judges that aircraft are going to get within that tolerance it will trigger generally a flashing alert, but TCAS as we said is I think, I don't know exactly, but is I think a hundred feet and fifty metres, so really close. So again, if you like a typical sequence could be STCA goes off, but for whatever reason you didn't act on or didn't see it and so on, so this situation keeps getting worse until it triggers a TCAS RA. But the example I gave earlier, STCA didn't go off.

R: OK, so there are cases where -

M: Oh, and if you do see the STCA then you'll perform some action or give some instruction that prevents an RA for happening.

R: So if I am following this right there are cases where STCAs are generated and no RA occurs, because the STCA takes a longer view of the distances and so on -

M: Yes, it gives the controller a chance to resolve the situation.

R: But there are also cases where you'll get a RA TCAS but not have got an STCA, like the case you give. Which was presumably because the physical separation was fine from an STCA point of view but something, maybe the climb rate generated it, because they have different logics.

M: Yeah, I think that's pretty accurate. It's all based on anticipated profiles, say for example STCA, I'm not sure of the algorithms and everything, but it might take into account the clearances or what the radar parameters; whereas the TCAS because it's aircraft to aircraft it's following a completely different setup, so you could have that scenario where STCA doesn't go off and you still get an RA.

R: I suppose the other question I would ask is are there any important aspects of air traffic interaction around the TCAS event that are missing from this model?

[time passes]

M: Well I mean unless you would want to add the, if you like the full cycle when the RA has been resolved; so say here `the pilot informs the controller for the RA', `the controller acknowledges' and it says `await resolution' - he does, but also you need to, so, one of the critical things with TCAS events is that you need to know when the aircraft stops being under my control and when it's back under my control. So that's why as soon as the pilot goes `TCAS RA' I'm like OK, that's me; I'm not going to issue any instruction, so my response would be Roger, and report back under my control.

So it's like a contractual thing; the pilot says this contract is now broken, I need to comply with this and then actually we reissue this and I'm back with you, I'm able to take instructions now. You need to be very clear about; the last thing you want is that box that you've got there [unclear what this refers to] that you try to issue an instruction while the pilot is complying with an RA and he has to tell you that he can't comply with it because of an RA and that's kind of the worst case scenario, because then your perception of what's happening might be different, your situational awareness is broken – you think that guy is under your control but he isn't.

R: So you need to have a good awareness of who is responding to the RA and is not under your control, and when they are back under your control so you can manage them again?

M: Yeah, exactly. I think that's the, one of the more vital things – you need to be very clear as to whether the aircraft is under your control or the pilot is doing his own thing to comply with the RA. And this is the same with things like weather avoidance or even when you have traffic services outside controlled airspace, where a lot of the traffic is unknown so you have different levels of service and there are different contractual agreements as to who is responsible for separation, or for looking out for the traffic etc. So I think that's one of the most important, the critical things to know when the pilot is under your control and when..

R: Can I ask one more thing, on the difference between controlled and uncontrolled airspace? Do you ever get problematic situations on that crossover point; say someone is, some levels, height levels of airspace are controlled and some aren't and you might have someone ascending or descending into controlled airspace…

M: You mean at the boundaries and so on? Well, potentially you could… To try and be as simplistic

as possible: controlled airspace is a predictable environment where you know what's in there, what's coming and your following certain clear rules and agreements between sectors and units etc.; then uncontrolled airspace you know it's a lot more unpredictable, pilots don't necessarily need to talk to anybody; you could fly in your little glider, your balloon, your all sorts in uncontrolled airspace and not necessarily be talking to anybody and nobody is giving you instructions, the pilot's just flying and doing their own thing, but of course you many have say an airliner joining from an airfield that falls outside the airway structure and wishing to join, so there is a portion of that flight where they are flying in uncontrolled airspace; yeah, potentially but this is the thing, why you have different levels of service, if you want me to go through them. You have a basic level of service which is basically information, there is no instruction issued, there is no traffic called -

R: So things like weather forecasts, -?

M: Exactly. Yeah, just saying, that sort of information. Then you have what's called a traffic service, which is I'll tell you what I see on the radar, there's something out there – I don't know what it is, I don't know what it's doing, if it's talking to anyone or not; I mean I'm trying to simplify here, there are ways of knowing whether he is talking to someone or not, but the point is it is unpredictable, so I can see something there, I give him 12 o'clock, range six miles or whatever, and it is the pilot's responsibility to avoid that traffic; you don't issue an instruction under traffic service, you only give information. And the next one is called Deconfliction Service, which means that the controller is providing instructions to miss the traffic, that unknown traffic, so you give the traffic information and you would say something like `if not sighted, turn right', or `to avoid, turn right' and so on; so you do give instructions, but it is still an unpredictable environment, so the aircraft you think you are missing might suddenly do an 180 degree turn and come back and chase you; so it's a bit more flexible environment where you might downgrade the service and say 'look I can't provide the separation – there's something that's going to get very close to you and I can't provide separation-

R: If you have some kind of confusing picture, where you can't quite follow the movements of other aircraft and say well, there are things here and things here but perhaps you should go right, but I can't guarantee it…

M: Well, exactly. It's a very unpredictable environment, you have all sorts of limitations and constraints; you may have aircraft that are primary only so they are not showing any squawk or callsign, just a little cross on the screen that could be a cloud, it could be a weather balloon or it could be an aircraft there, so you have no idea. Then you have, even when you have the secondary return you might only have a squawk and no height indication, no Mode Charlie, so you can only say that something is there; it could be well above you, well below you or it could be at the same level but you don't know, etc. Again, it's a very unpredictable environment so all you can do is, the best you can give is your best guess as to what is happening and you come in to this contractual agreement about what level of service and responsibility, how we are sharing that responsibility, which I'm guessing is what you guys are looking at. I think I'll stop there.

R: Now we'll go and look at another of our sub models, so I'll close down this one and now we'll look at some of the behaviours involving the pilots.

[Opens Pilot submodel]

R: So it's all sort of clustered around, I'll just zoom it out a little, shrink this down a bit – there we

are. These are the interactions directly involving the pilots.

[time passes]

R: If you wish I can turn off these sources, to make it clearer. Just get rid of some of the lines

[turns off Sourcing Layer]

[more time passes]

M: OK, OK.

R: So firstly, if you could, if you could describe each bit to see if, to see how you interpret the model and see if your interpretation is the same as mine. If you could very briefly describe each bit…

M: Yeah, it's funny like you say that the manuals `respond within five seconds' or `respond within 2.5 seconds', get this [unintelligible] out and see if, you know…

Yes, so these are two main TCAS events you can have – the traffic advisory, which means there is something relatively close so you just to look out for the aircraft and see that it is not a worsening situation, and the RA where you respond promptly…

`Ensure safe flight' - that's vague enough to…

See and avoid, yep…

What do you mean `update location and monitor RA'?

R: Yes, so..

M: Is that in relation to the conflicting aircraft?

R: Let me see where that came from…

[turns on Sourcing Layer]

R: Yes, so we got this from Chapter 5 of the manual. I think that was basically the sort of the pilot not flying having a duty to sort of…; while the pilot flying is doing the actual manoeuvre, of keeping track of the plane's location, of keeping track of nearby aircraft, the state of the RA – presumably to avoid the case you say where you say making it unnecessarily worse, by you know diverting from being in the path of one to being in the path of another.

M: Yeah, because this is the thing – the TCAS screen gives you a range of response that you have to follow and also the pilots' have the screen that displays where aircraft are and so I believe the TCAS might even point out the aircraft they are avoiding but you've got it there `see and avoid'; that's a basic flying principle. I think that sort of makes sense that the pilots won't just be looking at the screen but looking out the window and like you say – if they see the aircraft they are avoiding they can take further action, like a turn for example and also I think it is in some way a reassurance that you can see what is happening on the screen and also see that aircraft and judge that you are going to miss it.

R: So, that sort of spacial awareness that you; that the instruments are telling you the same thing as your eyes.

M: Yeah, I think it's probably that sort of confirmation as well, yeah and just awareness of what is happening – I think it is a different thing to avoid a dot on a screen than actually see a big chunk of metal in your vicinity.

M: Yeah, I guess interesting like you said `Avoid Manoeuvres contrary to RA'; I think also not just contrary but that might affect the RA: again, something like a turn – obviously an RA doesn't give you a turn instruction, but a pilot might choose that a turn would be appropriate to solve the situation quicker, or there might be other things going on; for example, you see the aircraft, you can see maybe that, they may be tempted to turn to get a better look at where the aircraft is, but also that might affect the RA; I'm pretty sure the whole thing updates if you are not compliant with the instructions then it will give you a new instruction or update… -

R: We'd sort of imagined, almost by default that when the RA is going on the pilots are making these vertical adjustments, and basically in horizontal space they go straight ahead as they also did; are you saying that sometimes the horizontal adjustment is also -

M: You'll have to ask a pilot for that, but I can definitely contemplate that scenario, where pilots would not just comply with the RA, but use their experience or context to help them; so on a clear day like this or in a clear environment they might want to look at; if they are flying in cloud they might just not bother in that scenario. Yeah, I can definitely see that as a possibility that they would carry out actions beyond what the RA is saying.

R: Again, that's exactly what this, this behaviour that is not written down in the manuals; at the same time seems to be a useful response to the.. scenario.

M: Yeah, I think it's good that the element of team work, or TRM as it's called in the manual; yeah, one pilot might be in charge of complying with the RA, but the other might be supplying more information to increase his awareness or trying to resolve the situation quicker; or like I said earlier one pilot might be, not necessarily the pilot that is flying the aircraft is communicating with air traffic for example.

R: So, in your experience the rather strict allocation of roles between the pilot flying and the pilot not flying is a little less strict in practice, at least in comparison to this manual that we looked at.

M: I would say so. The other thing I was going to say is that in these sort of extreme cases things tend to be a lot more strict, so the RA well you just comply with that, forget about complying with any other instruction; you just get the instruction so you can resolve the situation and like you say the; I'm not entirely aware of what the ACAS manual says but it might be the pilot flying that first gets the RA has to comply with it that tells air traffic etc. and then there's all these steps that we covered earlier; I think it's a bit like, in air traffic where we have this phrase equivalent to what the TCAS does, we have the phrase `avoiding action' which is to get aircraft moving quickly to avoid a loss of separation, so it's a very defined phrase, so it's avoiding action, turn right or left immediately, and then you give traffic information and you're supposed, I think it even tells you in the book "with a sense of urgency in the voice" - it's very…

R: Very detailed instructions on how you are meant to…

M: Yeah, and what I was going to say is that part of your training is that we going in to the simulator and practice these avoiding action scenarios, where you have to say many times and what

the simulator does is put aircraft in conflict all the time so it kind of becomes a reactive response where you get the STCA, flash, and then you have get that line out and come up with a turn that would, you know, make the aircraft miss. But interestingly, where the avoiding action that we give is always in the horizontal plane and it's because of the RA – you don't want to give an avoiding action in the vertical plane and then subsequently or simultaneously get an RA so this quite an interesting -

R: So you are doing that deliberately to avoid this conflicts?

M: So this quite an interesting point, that from an air traffic point of view in the extreme case that two aircraft are getting very close we give an instruction in the lateral plane, whereas TCAS gives it in the vertical plane, so in a way; it is clearly trying to avoid any conflict in the instruction.

R: So you avoid, in terms of, try to avoid, you give them in the horizontal plane, but, therefore instructions in the vertical plane are only go this to this airway, reach this height – normal operation, while the horizontal ones are; -

M: Not quite – it's just for that extreme scenario where you get aircraft that are very close together that we're not supposed to use vertical instructions; and I believe it is purely for this TCAS implication; of course normal ops we are turning, descending, everything.

R: OK, so basically if, that the instructions could end with two aircraft at the same flight level or similar; they would only occur before you though there was going to be some sort of incident, some loss of separation; so you might say; I'm trying to think of examples where aircraft have been assigned to the same flight levels and that has led to a direct collision or some loss of separation, but that would only occur when you didn't think there would be a potential incident.

M: Yeah, it's not a simple as that. You've gotta think that aircraft are crossing levels or we often say `exchanging levels' all the time; you have an airfield here and there are aircraft taking off and aircraft landing so they are going to be crossing levels all the time, so it could be that they cross that level you know a bit too close, or you know the performance changes or they might need to avoid weather; there might be a human error, or it could be anything really; the pilot could totally stop the vertical profile for whatever reason, so I think there are countless examples of why two aircraft might end up at the same level, but generally that what we're there to do, to avoid that scenario.

One thing I was going to mention earlier is this sort of extreme scenarios the manuals tend to be very clear cut and responsibilities are very specifically allocated – I do think there is a degree of flexibility, even in these extreme cases; I'm trying to think of an another example, but definitely in the normal operations their responsibilities overlap massively.

R: So again, are there any aspects here that you think are perhaps not especially relevant or are there any that missing, based on your understanding of the interactions with the pilot?

M: Yeah, like I say you would have to ask a pilot to get the full understanding, but to me it seems fine. Maybe just the wording – where it says "Do not follow ATC, if contrary to RA" it's actually prioritise RA over anything else, almost.

R: So like in that case we were talking about doing the horizontal manoeuvres, you may end up following the RA and also following ATC in effect at the same time?

M: Well, possibly, yeah, but I would say that in the case where air traffic's given a turn and then subsequently an RA is triggered the pilot could well stop the turn and just go with the vertical, or he might continue…-

R: So it's not quite so clear cut as the; they will absolutely, 100 percent drop the turn?

M: Yeah, exactly.

R: OK, that's very good, thank you. So the last of our, the last of these submodels is some of the interactions around the logic of TCAS itself.

[open TCAS model]

So again you can see the auto-reporting system that doesn't seem to happen is there and you have the rest of the logic.

M: I wonder if the TA notification would be between the TCAS and the generate TA…

R: Ah yes, you means in terms of the…; it's just sitting there for layout purposes.

M: OK, I see what you…

R: As you'll see later when you see the whole model it's densely laid out.

M: Yeah, OK.

R: So this does seem to be a relatively accurate description of how you would see the TCAS system operating?

M: I think so.

R: In that it does broadly seem to correspond to what you'd expect; are there missing elements or interactions that you would expect it to be involved with that you do not see in the model?

M: No, I think that is fine. I was just wondering the cycle of the TCAS with another intruder as you called it..

R: Yes, we have a rather simplified representation; it makes us think that all the stuff that happening here with this TCAS is also happening over here with the other unit, but then of course you have the case of the three-way and so on, so we only have it once, even though the same thing is replicated across any number of intruders.

M: OK, that makes sense.

R: OK, that's good; that's relatively straightforward. This is the point I suggest we take a break, have some biscuits…

[End of first half of interview]

R: So we saw the last of the separate models, so for the second half of this we'll first look at the full system wide model with all the bits you saw earlier plus some peripheral parts and then we'll look at some of the analysis results; as I said one of the important contributions of these techniques is when you have a model you can also generate warnings, notifications, alerts to potential vulnerabilities and look at those and see do these results from the model match real-world scenarios, or are they irrelevant in some way; are they an artefact of the model problems, rather than problems in the real scenarios. So let's open up our model…

[Opens full model]

So you can see why I did the sections first…

If you just take a minute or two to look at that, then if you could sort of talk, describe what each section appears to say, appears to describe so we get this idea of how understandable the model is.

M: Yeah, so you've got the actors involved in an TCAS event in some detail there, going to back to the regulator and the manufacturer and so on. And you've got TCAS there is an actor, which I think is quite interesting to see it that way, the processes it's going through; in a ways it's also making decisions – the kit itself is providing instructions and sort of part of the cycle if you like; it's also interdependent so it depends on what the pilot is doing with the aircraft and TCAS will update with that…

R: Yes, one of the reasons we model it with a bit of detail is it's interesting what happens when say one of these parts fails and we see what are the implications of that, rather than just treating it as a black box that sits there and does things.

M: Yeah, I mean because, yeah, it does happen that say aircraft, they're actually allowed to fly without TCAS for a determined period, I think it's ten days but um, I'm stretching my memory but I think it is ten days – you know, it does have a lot of implications even to how you handle an aircraft that doesn't have TCAS for example, so I think it is quite good that you've included it like that, as you say that level of detail.

R: Is that something that you do encounter, that there is an aircraft that should have TCAS but doesn't?

M: Yes, and pilots tell you that their TCAS is not serviceable, or in the flight plan or strips you receive you have a note, so if it's something they knew before taking off they will have a note in the flightplan so everyone knows, but if it's something that's happening in flight, they get an error message or something they tell you; and it does vary how you control the aircraft, because say we focus in this model on the case of resolution advisory but also the traffic advisory, again with the sort of situational awareness I'm not sure how often, how commonly they go but it's something I'm sure they get all the time and it doesn't necessarily imply that an an RA is coming – it could, but a TA is just saying there is something close by, you have a look and assess the situation a little bit, see if there is anything that you might want to do or need to do; a pilot might respond to a TA just asking the controller, saying "We've got a traffic here showing." Remember I was saying outside controlled airspace earlier – so if I haven't told him about an aircraft and he gets a TA, he's like "that looks a bit close, I'm not entirely worried" but I'm flying here outside controlled airspace so I'm going to ask the controller and see what he can see on the radar. So it does change how you

operate to an extent; it doesn't, I don't think it's a major change but you might say for example as a controller provided a bit more traffic information to an aircraft that doesn't have TCAS because you know they're not going to get this notification if you like; I'm not entirely sure, I think, the TCAS not working also affects the display they have, cause the TCAS has a little display with other aircraft in the vicinity so it might be that that display is not working at all so they loose that little bit of awareness; you might compensate for that as a controller.

R: So the interesting subtly there is if they are flying with TCAS inoperable for some reason that puts more load on you as a controller, because you need to give them a little bit more information to compensate?

M: Yeah, I mean it could be. It's something that it's not like you are required to, but it's something that keeps things flowing nicely and you know, it's something that could have safety implications quite clearly, so you do try to compensate a little, like you say.

So then well, the rest. You've got the pilot flying which we discussed earlier about why you decided to make that distinction, but I mean, for me I think, I'm not sure again, you would have to ask a pilot there, but to me I'm not entirely sure if that distinction is so black-and-white; so it has those clear boundaries. And this is purely from my experience, because likewise in air traffic we often what we call `singleman' so there is one controller in charge of the sector, but quite often we have tactical and planning, two controllers managing one sector and we have again very clear definition of roles and responsibilities, but at the end of the day everything overlaps and if you go down the STCA route well it might be a controller not in charge of the radio, of issuing the instructions might be the one that points out, or you might see an STCA going off in a different sector, you might shout across or give them a phone call and say – look I've seen this, have you seen it? So, it's not if you like part of my responsibility to do separate aircraft in a completely different sector but if I see that happening I will take action to check that…

So, basically I think it's good, especially if that's how it appears in the manual ….-

R: That does not mean that it is true in any sense -

M: Yeah, but I would definitely try and dig deeper and see if that is the case for that clear distinction, because it does seem like the responsibilities have been allocated quite distinctively to the pilot flying and the pilot not flying, because obviously you have those roles pilot flying / pilot not flying are not the same throughout the flight, they are switching all the time and you have, if you like, the seniority or the -

R: Indeed, another aspect that we haven't said, again from reading the manuals it seemed that the idea of seniority was essentially irrelevant, but there are presumably at least social aspects in the hierarchy that… I read of cases where the first officer has noted some problem and tells the captain, and the captain says no "I'm right" and some nasty accident occurs.

M: Yeah, there has been a lot of work down along those lines and I think it has been clarified that to an extent even though you have the captain / first officer you still have a degree of authority to challenge authority if you like, or authority to challenge what's happening. So there is stuff there might have some influence, but to me I would look at a bit more what happens in reality in these scenarios, in terms of pilot flying / pilot not flying.

R: Perhaps now I can ask about – you've already seen these bits, to have a little look at how they overlaps. Firstly, for example, we have – I think we covered most of this earlier, but the air traffic control and the pilots interact. So you mentioned for example that you need the pilot to inform you when they have finished responding to that, that is covered. Are there any other interactions in the timeframe of about to get an alert, I get an alert, I resolve the alert that are perhaps missing from the interactions directly between the pilots and the air traffic controllers.

M: No, I think we discussed most of it. There needs to be that clear switchover point where the aircraft is under the control of the controller and when it is following the RA and from the point of view of the controller like I said earlier maybe provide additional information to help resolve the situation or to limit the impact it may have in the extreme case, but there could be another scenario where another impact by following an RA you might have to do something else, most likely with other aircraft but possibly with that aircraft.

R: So having dealt with one aircraft you may have to move all the others around it?

M: Yeah, absolutely.

R: I suppose I come again to the question of are there, now you've seen everything we've modelled, are there important issues missing, areas missing, that you would consider to be relevant in this kind of scenario?

M: Not really, I think; I would have to think about it a bit – we just discussed a bit about the levels of detail that you would go in to and how much you would expand it – there are obviously knock-on effects if you like from this sort of event; from the point of air traffic we discussed about maybe you have to move other aircraft out of the way, or maybe you have to coordinate with some unit for example, or; I'm thinking for example in providing that extra bit of information to the pilot that's following an RA, so I mentioned earlier saying "this is known traffic that you are conflicting with" and say the other aircraft is also under my control, could be under my control so… It's not exactly reassurance but it's a way of keeping them in the loop of what's happening; it could well be an infringer – an aircraft that I know nothing about it's just infringed controlled airspace, flying into this other aircraft and got an RA resulting from that and I would tell the pilot – well, this is unknown traffic, I don't what it's doing so keep a really good lookout because there's nothing I can do here to help you; whereas if it's an aircraft under my control already I can just say well, dunno get him out of the way or give him traffic information, to let both pilots know about each other – this sort of thing, but…

R: So the added complexity there when the infringing aircraft is not under your control, and that's a more complicated scenario than when you're dealing with aircraft you all control. Does that sort of scenario occur regularly or is it a fairly unusual thing?

M: Well I mean an RA already is an unusual thing, so within RAs you would have go to the safety publications like the Air Accident Investigation Branch, they publish all the records yearly I think; so you'd have to look for RA events and see what the contributory factors were – it could be infringement, -

R: So it's not something that's happened often enough to you yourself to -?

M: I have seen it, I have experienced it but in terms of RA – well I dunno how common or

uncommon it is in terms of RA events; I wouldn't dare guess, but it's definitely possible, something I've seen, infringers do happen, I couldn't say how regularly, but it's not something extremely rare that only happens a couple of times a year. Does that make sense, what I'm saying? When an RA events happen there's like little flakes of things that you might have to act on, but it's not something that you would exactly see in a manual; it's not exactly something that would happen all the time, but more like specific to each RA scenario.

R: So basically you have to rely on your general experience, rather than following some procedure that has been written down for this particular case?

M: Well there's definitely that, but I think it's more the specific, the specifics of that scenario, each particular scenario that would say influence what other actions you might take. If that makes sense.

R: So in the context of the particular incident?

Which obviously makes it more difficult to write down and model?

M: Yeah, that's what I mean that it's; I'm not suggesting that you incorporate all of it, but it might be just a generic branch of saying `Assess further impact', because your goal might not just be to resolve that one scenario, but actually assess the impact of that one scenario. If we can go back to the example of the holding stack you might not want to just resolve that one RA, but if there is massive knock-on effect like five, six other aircraft are going to get an RA you may have to, you could take some action that limits how many dominoes are -

R: So we know that an RA is generally a disruptive event and you want to minimise the effects that go on?

M: It's interesting the dotted line – I didn't know that the TCAS could have the function; it might make sense, maybe Datalink or…

R: Yes, that was the idea.

M: But, it's always a fine line as to how many alerts you can incorporate in a system before you go under with ten alerts going on at the same time…

And also, in terms of the controller if anything it would clarify what we talked about, saying well this aircraft is receiving an RA and isn't under my control right now; I think you'd rather hear that voice saying `this is what's happening' than just see the alert and hear nothing and the aircraft is doing some deviation from the profile.

R: So you'd rather get a direct conversation with the pilot rather than rely on another layer of computer supported-

M: Yeah, yeah. Because also you cannot miss the pilot talking to you but you can an alert; or an alert might be spurious but the pilot will never tell you he's following an RA when he's not. [laughter]

R: Yes, the pilot's not going to malfunction and say…

R: Right, do you have any more comments on the model before we go on and finish up by looking at the analysis results we have generated.

M: No, I'm actually interested to see that next stage. Are you going to talk through examples of how to apply them?

R: Yes, I'll talk through them rather than just presenting them rather than just presenting you with them…

So I think we have about four or five techniques that apply to this model. In that case I need to bring up the analysis window, so we can see more of them. Warnings and information points.

OK, so possibly the first one we should look over is this idea of reliance; so the idea being that, it comes back to the situation we showed in the little restaurant example where you're held accountable, you hold some responsibility and you rely on others to help you do that, the way the restaurant manager relies on the waiter and the chef. And if they are not there the tasks of the restaurant manager will fail, even though they have not done anything wrong themselves. Therefore, what we do with any model this reliance technique just generates lists for each actor of who they rely on. And perhaps we can look through these and see if they look like a reasonable way of understanding the relationships between the different actors. So I think we have five of those – if you hover over the actors you should get a list.

First one is we say that the Air Navigation Service Provider relies on the ATC staff. Does that seem a) truthful and b) useful?

M: Still within the RA scenario?

R. Yes. Although, some of these more general responsibilities broaden it out a little.

[time passes]

M: Yeah.

R: Perhaps a more interesting, a more complex one certainly is if we look at the pilot flying (PF) then we see that they rely on air traffic controllers, they rely on the TCAS system and the manufacturer of the TCAS system and they also rely on their colleague the pilot not flying. Is that an accurate representation of the kind of thing…-

M: Well, I think in terms of an RA I would sort of question that they are relying on the air traffic controller during an RA – it might be specific to each scenario because it might have been human error on the side of air traffic or some other thing, but really like an RA just takes the responsibility straight on the pilot, so he doesn't require an ATC to act on that RA if that makes sense.

R: That's a fair point. I think the reason it's generating that particular alert is I think from the part of the duties when responding to alert, informing the controllers. If there is no traffic controller to inform then they can't do that. But I see your point that during that particular subset of time they're basically on their own.

M: Yeah, and also what you find sometimes with RA events is that the pilot only tells air traffic once it has been resolved; clearly his first duty is to avoid hitting another aircraft; I mean the pilots call it, I forget - "Aviate, Navigate,..."

R: "Communicate"?

M: Yeah, that's it. So fly the thing first, then navigate to where you want to go, then tell other

people what you're doing.

R: So sometimes the first you hear of it is "I had this and it's fixed"?

M: Sorry?

R: So sometimes the first thing you hear of an RA is "I had this and it's finished"?

M: Yeah, that could be. I would say that's relatively common, I mean it's something – they go 2.5 seconds or 5 seconds..?

R: I think it's 5 seconds, then 2.5…-

M: For the first response, but if they can do it in 2 then they'll do it in 2. So it is relatively common that they go "I've had an RA, I've resolved it, I'm back with you". Sometimes you might not have noticed at all. So this is kind of why I'm saying; I see your point that it relies on ATC at least acknowledging they're going through an RA, but at the same time even if ATC say nothing, do nothing, don't hear or whatever – they're still going to do it.

R: OK, and we mentioned earlier the rather complex interaction between the pilot flying and the pilot not flying which covers that part.

M: I see what you are trying to establish, like dependencies and that, and the pilot is kind of overloaded with relying on all these different people.

R: Yes, I think the broad conclusion that I got by looking at this is, which is not in any sense a difficult one to reach is that is it's a very complicated, inter-related system where everyone to some extent depends on everyone else; if there was no air traffic control tomorrow there would be a big crisis and it would…

M: It's interesting, because you know, you might know more than me by now on TCAS; If I remember part of the history TCAS was developed for aircraft flying in remote areas with no radar for pilots to avoid each other – that means no air traffic, pilots still do their thing, avoid each other; so again it might…

R: That's absolutely true – I think it was the case of the American Mid-West where it was just wide open spaces…-

M: Flying through desert and so on – basically non-populated areas, so kind of what I'm saying is that air traffic in this particular scenario is not irrelevant, but not like a massive actor; it's almost like you say, cut here, cut here – in this brief moment of time you are on your own and then you reconnect to what you were doing thirty seconds ago.

R: That's interesting, in that TCAS was first developed as an idea at least you had these large areas of uncontrolled airspace…

M: Yeah, exactly – basically no radar coverage. You have in air traffic what's called procedural control which doesn't require radar but relies on pilots reporting; I think an example like the Sahara desert so an aircraft flying west to east is not talking to anyone, there's no radar cover there and basically he's just see and avoid like you've got there – so TCAS brings a level of detail or awareness that wasn't there before and allows pilots to avoid each other in this sort of area.

R: Is that also sort of true of large oceans, presumably there isn't radar because sea rather than land?

M: That's what I was saying – it's procedural control, it relies on pilots reporting where they are and what they're doing – so you'd clear a pilot to cruise at a certain level and pass your degrees of longitude at certain points at a certain time so you have time separation – ten minutes or something, where the aircraft says "I have passed twenty degrees west" and then the next aircraft has to pass that ten minutes later at the same level, or maybe a different level – there is still control because you can tell an aircraft to climb or descend, you can still issue instructions but you are not seeing them on the screen.

R: In that case if one of the aircraft becomes disorientated then you can't tell that, if they go off course...

M: If they don't tell you you cannot spot it.

R: So if they don't know they're off-course then neither can you?

M: Yeah, yeah.

R: We've made the assumption that in this model that basically everything is happening in well-controlled airspace; radar coverage and everything else, and not so much either uncontrolled or the procedural stuff where you're reliant on accurate information being provided to you in order to generate accurate instructions.

M: I mean, I think this scenario would work anywhere, but I think it's just that secondary role of air traffic because the secondary, well like I say it becomes bottom of the pile.

R: We're focusing on the exact moment where there is an RA and something has to be done, but do you think that the idea that the pilot should inform the air traffic controller maybe comes from the fact that the air traffic controller can they look at the rest of the aircraft in the area and start advising them as soon as possible that something is going on and that they should make space?

M: Yeah, exactly.

R: I suppose a version of that is – would you prefer when an RA occurs to be told as soon as possible, or…

M: I prefer ASAP.

R: Let's look through more of these reliance relationships. Let's try another simple one – the aircraft operator depends on the pilots to… not much to say about that.

So let's look at perhaps the most complex one of all – the air traffic controller themselves. And they rely on the pilot flying; interesting we go back to the same point you made earlier – we don't have them relying on the pilot not flying, which is a more subtle issue than it looks; we have them relying on their short term alert system and we have them relying on TCAS, which I suspect is not something you would think?

M: Yeah, it's kind of indirect relationship where you were talking earlier; it's because the TCAS through the pilot – we don't have a link directly to TCAS.

R: Do you find yourself, for example when responding, dealing to an alert and find yourself

thinking in terms of the TCAS logic, trying to work out how this happened, or is it more "well this happened, I have to deal with it"?

M: Well, I'll give you an example I think I might have mentioned – TCAS is designed to avoid a collision, but it also provides the traffic advisory, so there was this incident where an aircraft was cleared below another one and so he was like a safe, normal clearance but the aircraft was climbing, and so responding to a TA actually started if I remember correctly he was looking out for traffic above him and what he ended up doing is what we call bust the levels; so he went beyond the level he was cleared to because at that point he wasn't complying fully with the instruction but he was actually looking out for the aircraft above so he ended up – the controller lost separation, the pilot failed to comply with the clearance. So this is an example of how air traffic also rely on the TCAS just in this RA scenario, just through the use the pilot makes of it.

R: So the pilot was looking at his TA notification and making actions based on that, and they were getting other instructions from the air traffic controller that didn't match?

M: Not quite. I think the focus went away from the instruction to just looking out for that other aircraft, and could well have been; I can't remember this, but anyway it could have been the controller actually gave that information – climb to this level and be advised there is another aircraft right above you, a thousand above that level I have just given you but that didn't; the pilot he was like well there is something above me, where is it? and didn't realise he was going past the level he was cleared to, which resulted in an incident even though if you like safety wasn't compromised because the pilot was "Oh yeah, there he is"…

R: So basically he was alerted to the fact there was an aircraft above him and he wanted to be able to visually see it so he kept climbing until he could see it?

M: I'll give you an example – it's like you're driving on the motorway and your following this car which suddenly accelerates and ends up doing 100 miles per hour; you've just been following it at a safe distance, but suddenly you're breaking the speed limit. Your task if you like is drive safely, but is also don't go beyond 70 miles per hour; but here you were driving safely following a car but actually you ended up busting the limit.

R: So that's more like both planes were climbing?

M: No, this one was in level flight, but the one above was climbing but is started separating itself not by the air traffic separation standards, but by him visually looking at the aircraft above.

Also, this visual separation exists near airfields so it's whether there's air traffic or not pilots say "I will maintain my own separation with this guy because I can see him and I can follow him or avoid him" and at that point the air traffic controller is discharged from that separation, if you like. But I think the driving example might not be a bad one to use.

R: So in the same way; you have the separation as the controllers would define it; you've already mentioned that the definitions that TCAS uses are different and again the parameters for what the pilot thinks is visually safe are different again from both of those; therefore something that satisfies one or two of those will not satisfy the third one?

M: Yeah.

R: OK, so the next kind of analysis we generate out is about overload, whether or not particular actors in the system are potentially at risk of being overloaded and therefore having their performance impaired because they are trying to address too many responsibilities.

So for this model we have three different actors that are potentially overloaded; we'll just go through… Firstly, the most overloaded (in theory at least) actor are the pilot flying, because they have all these different responsibilities to handle. So the question perhaps to ask there is do you feel that is a problem in practice that the pilot has too many things to do at the same time during a response to a TCAS alert?

M: Hmm. You would have to ask a pilot! My sort of feeling is that you're probably right that he's overloaded with responsibilities but at the same time the minimum for him to resolve the situation as long as he's prioritising the situation to be resolved; a bit like I said earlier – the TCAS gives him a climb / descend rate to resolve the situation – as long he complies with that then everything else is almost like secondary; so yes and I'm still not sure it would impair the outcome.

R: So basically as long as they prioritise properly they should be fine?

M: Yeah, and I think the prioritisation is quite clear and it would be a purely reactive response; and also you have the imperative of the alert "Climb, Climb" so the whole sort of system is geared towards that resolution. Obviously I do agree that the pilot is probably overloaded, but I'm not sure it's to the extend that it would impair his ability to resolve the situation.

R: So I suppose the interesting question there is could you imagine a scenario where if something else happened during this, during a TCAS RA then there would be trouble? Say for example what happened if they were responding to this alert and had some sort of mechanical failure at the same time. Would that put them on edge?

M: Well, I think it is quite common that cockpits have tons of alerts for all sorts and obviously they have I don't know how many systems – quite a few, so I think it's relatively common or at least statistically very possible that several alerts go out at once, but I don't have exactly enough knowledge to know they how operate and maybe whether some alerts take precedence and so on; but I would say is that in terms of ATC this kind of event has potentially big implications because an aircraft deviating from its expected profile like I was saying with the other examples it might have a massive impact; like you were saying earlier you might have to take aircraft out of the way or update definite instructions or you might affect a different sector or a different unit – the ramifications can be quite big.

R: So this brings us on to the second overloaded actor, which is the air traffic controller which has substantially fewer distinct responsibilities in this model but still has quite a lot and so we get an overload warning. So as you're saying, is this a scenario where you feel that to respond to RAs can overload the controller, possibly to the extent of their performance – either to do with that or to other things?

M: Yeah, definitely. Because, I'm going to try and give an example – the one in the stack is quite a good one – you can imagine the knock-on effect of that might happens because you start having to phone other agencies, to start focusing on that one scenario and possibly neglect others developing around the sector and… Yeah I think the way, the job relies on you being able to exercise control

over aircraft, so whenever you can't exercise that control then you stop being a controller for one – but also it starts limiting how you can run the centre; the RA is a good example in the way avoiding bad weather is another – you basically not only loose control but you loose awareness of what's actually happening because you've heard the pilot saying he's following an RA – so what's the RA telling him? If it's a climb he is going to climb 1000 feet? 300 feet? 8000 feet? You don't know. Also, what else triggers that RA? It is because some unknown aircraft has come in? Because of a mistake I've made or a mistake another pilot made? Or what else are the implications?

R: All this uncertainty is introduced.

M: Yeah. It becomes an unpredictable scenario suddenly. I would say that's probably one of the biggest impacts.

R: I suppose one of the subtleties of this, the model doesn't capture is of course the pilot is only flying one plane, while you are controlling ten, twenty, some large number of aircraft, simultaneously.

R: The final example, which perhaps shows a limitation of the technique, suggests that the TCAS itself might be overloaded because it has to, the various alerts is has to generate, which I suspect is not something that happens in practice; TCAS units don't get overwhelmed by the number of aircraft or anything like that?

M: This is something we sort of cover hypothetically; so you could have a situation where the TCAS instruction, the RA is actually continue with level flying, because you might have aircraft climbing or descending and you're in the middle so it could be like, just keep level flight and it will tell this one to climb and this guy to descend, for example. So yeah but I mean, trying to think; trying to think of the parameters in multi-aircraft encounters.

Because the source of the…; I think there's been a couple of incidents like that; say you have an aircraft climbing and an aircraft descending – both through their levels, so they are going to trigger a TCAS alert. The TCAS might say to the aircraft climbing "Descend" and to the aircraft descending "Climb" - but say the pilot has visually identified the other aircraft and he's climbing and thinking "Well actually I am going to do this", and the pilot climbing can see him and say "Well I can see him, he's way out there so I don't need to descend" - I think the TCAS does update, but the first response from TCAS is to give you an increased rate of descent; I think it has not only climb or descend but also increase or decrease rates of climb or descent, it does sort of update.

R: So you have there potentially counter-intuitive instructions?

M: Well, I think that's a very good point – it is at least hypothetically the case that you could have counter-intuitive instructions, where the pilot might think they are better off climbing…

R: I suppose the real danger here in this case is that one of the pilots thinks this is counter-intuitive and won't follow it, and the other pilot thinks this is TCAS and so I must follow it, and so they end up on the same level.

M: I think as we've found already it's quite clear that the pilot should follow TCAS. But I can see how the TCAS itself could be overload because you could have multiple aircraft and the different degrees of response; I don't what the refresh rate is for TCAS but you could have a pilot that takes

six seconds in responding and the other could take ten; they comply in different ways so the TCAS does need to update that.

R: That's a good point – I have no idea how quickly it updates and can see that being an issue if people don't respond in the timeframes expected.

M: I think that is definitely something worth looking at.

R: Now we have what is called "critical entities" - that's our identification of vulnerable points of failure, where would cause the most failures down the line if they failed themselves. So this one is; there are three alerts but are basically all saying the same thing which is that in the model of this system the most critical element with the worst effects if it fails is the TCAS itself and the steps towards generating the notifications. What are your thoughts on that?

M: So the requirements for generating an RA, so you need to have both aircraft with transponders to get the height information and at least one of them to have TCAS: both aircraft don't need to have TCAS, but both need transponders to get the height information that TCAS is reading from; it's picking up that height information and their location so it is a vulnerable system in the sense that it could be an aircraft without a transponder or where the transponder is not working or might be incorrect – there a lot of things that could affect how effective the TCAS is; it's something that is not uncommon that the Mode C altitude is not working or might be erroneous or because it's based on the altimeter setting it might be off so there's quite a few parameters there. I can't think of another one, so it's more like the technical side of it rather than the social if you like.

R: So in that sort of case, where the TCAS is either not generating alerts or is possibly generating alerts based on incorrect information, such as from the faulty transponder – what are the implications for that for everyone else in the system? Is that going to put more and more effort on other people, is it going to lead to confusion or other undesirable effects?

M: Yes. I think all of those. It could definitely have confusion and if it's not generating an RA you're leaving the pilot and/or the controller to resolve the situation without the help of TCAS. So say for arguments sake that the controller spotted the confliction which is too late to resolve, then they can intervene and either give an instruction to avoid or tell the pilot "There's something really close, can you take avoiding action there"; or it could be the pilot spots it visually and takes a turn to avoid – from the controller's point of view he just sees the pilot taking a massive turn or climb. So I think the impact of a TCAS not correctly issuing an RA can be quite severe. And also because the parameters are to avoid collision with very tight margins, so potentially you could have a collision there which is the worst outcome.

R: So if there is a relatively small inaccuracy it could still be outside the margins defined; if it's off by a hundred feet or something?

M: Yeah, yeah I think that's a good point – that the tolerance that TCAS uses means that if whatever information is fed in is out by a certain margin then it could well have a pretty dangerous scenario.

One sort of occurrence that you get regularly is when you have aircraft not transponding, so not transponding the attitude – that generates a TCAS TA, which means that the guy could be anything from on the ground to five, ten thousand feet above so a pilot's response to that is querying us - "I'm getting a TA here, but what is it" and for me; quite often you can have what we call 7000

squawks – 7000 means that he's not talking to anybody, it's a way of saying that I'm here but not talking to anybody but you can still see; so that way you can say there this guy, it looks like it is low-level so should be well away from you, that sort of thing and give a bit more information, but if it was say a jet and you had this 7000 squawk with no height information and also fast moving then you start worrying a little bit, because you think it's fast moving and might go somewhere up down, it might be a military jet or something like that. So it does bring a degree of confusion when the information is like incorrect or incomplete – a TA regularly pilots would question it - "I've got some traffic here, do you know what it is?" and you're like "Yes, it's another aircraft under my control that's crossing underneath you" or something like that.

R: So in that sort of case where you don't have the full information, say from the transponder – is better to have say a transponder that it is on but doesn't have altitude information or is better to have no transponder which would be easier to deal with?

M: So the transponder essentially, I won't got into the mode S which is very detailed information; basically have Mode Alpha, Mode A which is the four digit code – the one I mentioned is the 7000 which means I'm not talking to anyone, I'm doing my thing, I'm here; then each aircraft can be assigned a four digit discrete code which is assigned to just that aircraft – that's what converts to callsign so you have codes for certain routes or certain airspace or certain airfields that once you see them that particular squawk belongs to that particular airport or you can see the callsign converted because it's linked to the database; then you have the Mode C, Mode Charlie that indicates the attitude – they're both part of the transponder but they are independent so a pilot could stop either of those two; obviously you can change the squawk to tell the pilot to dial a new code and also as a controller part of the duty is to check – we call it `validate and verify' - validate is the Mode A, Mode Alpha to check that the code was the one you expect and verify the Mode C, Mode Charlie – you get an altitude report from the pilot and you look at the screen, you check that it is what is says and you go it's accurate.

R: So the pilot says "I am at 8000 feet" and if the transponder says they're at 10,000 feet then you know there is some problem?

M: Exactly. So you query it, and then he might reset it or check the altimeter setting or switch to the other transponder if that's not working possible and basically that's what we use for separation, so it needs to be within a specific tolerance. I'm not entirely sure but I believe TCAS works on the same bit of data, so if it's off by a couple of hundred feet it could potentially be bad.

R: So I think that's us covered most of the warnings we get from our analysis algorithms – I suppose we've talked about the failure of critical items, parts of the system; we've talked about the effects of load, particularly on pilots and control and we've talked about the interdependencies between different actors. So I suppose what I should ask now is do you think there are issues in terms of loads or potential mistakes or vulnerabilities of any general sort that haven't been covered or mentioned by those techniques? Are there other sources of vulnerabilities that the model doesn't tell us but you do encounter?

M: Let me have a think.

I think from the ATC point of view it's pretty much covered. I can't think of any right now. We've discussed a few, but I can't think of any right now.

R: I suppose that's moderately reassuring that there are no obviously huge gaps in the model that are not being picked up – that's good. So I suppose that's basically then end of my list of things that I wanted to work through – so are there any last points you'd like to make about the model and the things we've discussed, or are there any questions you want to ask?

M: No, I mean – one thing is maybe identify the fuzzy boundaries that you might have – we discussed mainly the pilot flying / not flying but also things like the need to inform ATC or things that are not exactly always either clearcut or at least there isn't room for manoeuvre like those responsibilities being switched – the pilot flying non-flying is a good example I think – it's quite interesting to see that the pilot flying is overloaded, so you can see how in reality the other pilot will be taking over some of those responsibilities, so maybe identify those that are either in practice or in theory a bit shared or allocated more flexibly, I guess.

R: When the load increases on the pilot flying then it's natural to delegate away, transfer away?

Some things can't be transferred – they're physically flying the plane, but what things can you transfer and how that interacts with the regulations, by the book, you have to do it this way?

M: I think that's the only way, but the one thing I will mention is it's a judgement as to how much extra complexity you have to add…

R: This is the kind of thing…; we need people like you to tell us that reality is not as clear-cut as the books say; we're not going to find that out otherwise other than by-

M: The other one would be the hierarchy of those responsibilities, as we said with the `Aviate, Navigate, Communicate' well if anything happens then the first one you drop is this one, and then this one and your ultimate priority is this one.

R: That's a very fair point, because all of these are basically at the same level of priority – we don't have a representation saying well do this but only if you've done these other things first, which in reality-

M: Yeah, I think that would be an interesting point – I don't know how you would implement it with sort of colour-coding or numbering but it would be interesting to add that extra information of what is the most important thing here or what is the critical responsibility here.

R: We have a very basic way of notating this; you can do one option or the other. We've got the idea that prioritising is important and we should record that, but haven't quite got to the point of thinking through the implications of that in terms of our analysis. There are clearly very interesting effects – if you do one thing before the other then perhaps the second one is delayed somewhat and some cases will take longer to perform than others and in some cases that has effects on subsequent actions.

M: Or at least what sort of responsibilities are not critical or if they are dropped the goal is still achieved sort of thing.

R: A sort of must-haves and nice-to-haves?

M: Well they are all there in the manuals so they are must-haves but even within the must-haves there are some things that are still more important.

R: Yes, I mean it’s more important that they don’t crash rather than that they tell you?

M: Yeah, that’s definitely a clear one.

R: Any last comments or will we wrap up? Excellent – than you very much, that’s been extremely useful.