Understanding the Interaction between Safety Management and the ‘Can Do’ Attitude in Air Traffic Management: Modeling the Causes of the Überlingen Mid-Air Collision

Chris W. Johnson,
Department of Computing Science,
University of Glasgow,
Glasgow, G12 8RZ, Scotland.
+44 141 330 6053
johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk/~johnson

ABSTRACT

This paper focuses on the contribution of Air Traffic Management to the Überlingen mid-air collision. Events and Causal Factor models are developed to show the interaction between technical, human factors and managerial issues in the causes of this accident. In particular, we show how problems in safety management contributed to an error inducing context. Our analysis also points to the wider dangers that arise from a ‘can do’ attitude in which staff actively device ‘work arounds’ when faced with a degraded technical infrastructure.

Keywords

Accident investigation, ECF modeling, Air Traffic Management.

INTRODUCTION

The Überlingen accident occurred on the 1st July 2002 when a Boeing 767-200 was involved in a mid-air collision with a Tupolov TU164M [1]. A total of 71 crew and passengers were killed on both aircraft. The immediate causes of the accident centered on the Air Traffic Control Officer’s (ATCO) instruction to the Tupolov crew, which contradicted the Traffic Alert/Collision Avoidance System (TCAS) on-board warning system, and ordered them to descend into the Boeing 767 which was also responding to a TCAS warning to avoid the other aircraft. This accident had wider repercussions and prompted international initiatives in Europe and the US to reexamine the causes of mid-air collisions. The following pages form part of these initiatives. An accident modeling technique is used to identify further insights from the original BFU investigation. The report into the accident was issued in 2004. It provides a relatively thorough analysis of the causes that led to the confusion over the warning from the TCAS software. In contrast, this paper focuses on the infrastructure changes at the Zurich Air Traffic Control Center. Scheduled maintenance procedures created some of the preconditions where the ATCO was likely to make a mistake

THE CONTEXT FOR THE ACCIDENT IN SKYGUIDE

Figure 1 uses a simplified form of Events and Causal Factors diagram to analyze the background to the Überlingen accident. This notation was pioneered by the US Department of Energy and is one of several alternate formalisms that might have supported our analysis [2]. ECF was selected because it provides a graphical overview of the events leading to accidents and incidents. It is also recommended by organizations, such as NASA, for use in the analysis of aerospace accidents [3]. Ellipses denote contributory factors that combine to make events more likely. Events are denoted by rectangles. The figures in parentheses refer to the page numbers in the BFU report that contain information about these contributory factors. In the following diagrams, some events are annotated with ‘Ass’ to explicitly represent any assumptions that were not explicitly referenced in the BFU report.

Skyguide had only recently been formed (in 2001) as the successor of the former state controlled ATC "Swisscontrol". Hence, although the organization was relatively mature it had to face a new commercial ethos. The staffing difficulties were compounded by a European shortage of qualified Air Traffic Control officers. The company also had to respond to national and international encouragement to create a Safety Management function within the organization. This encouragement led to the publication of the Company’s Safety Policy in 2001 that, in turn, required the development of a Centre of Competence. However, as can be seen from Figure 1 staff shortages delayed the development of this Center. Although existing strengths in areas such as internal audit could still be relied upon there was little background in risk assessment. One consequence of this was that in the lead-up to the Überlingen accident the risk manager was not informed about the planned sectorisation work. Hence, the ECF diagram draws a direct link between high-level judgments and often very ambiguous statements about the importance of ‘safety culture’ and the detailed events that led to this collision. In this case, we can trace a path directly from the need to meet national and international guidelines of Safety Management Systems through difficulties in staffing to meet the Company’s Safety Policy to a failure to inform the Risk Manager that ultimately explains why there was no adequate risk assessment of the sectorisation work.

The importance of the analysis in the previous paragraphs should not be underestimated. As we shall see, the lack of risk assessment illustrated in Figure 1 had profound consequences. It may have prevented staff from understanding the potential consequences of the sectorisation work that took place on the night of the accident. This work deprived controllers of key elements in their technical infrastructure [4]. The organizational factors illustrated in this first ECF diagram can also be used to explain why a single controller was left at the workstations on the night of the accident. There is the obvious connection that staff shortages had led to two members of staff being rostered rather than three. The delays in establishing the Center of Competence and the lack of background in risk assessment, arguably, explain why there had not been any thorough risk assessment of Single Man Operating procedures even after there had been two previous AIRPROX incidents in ACC Zurich. The delay in establishing the Center of Competence may also explain problems in establishing the types of incident analysis capability that would ensure a more complete risk assessment in the aftermath of previous adverse events.

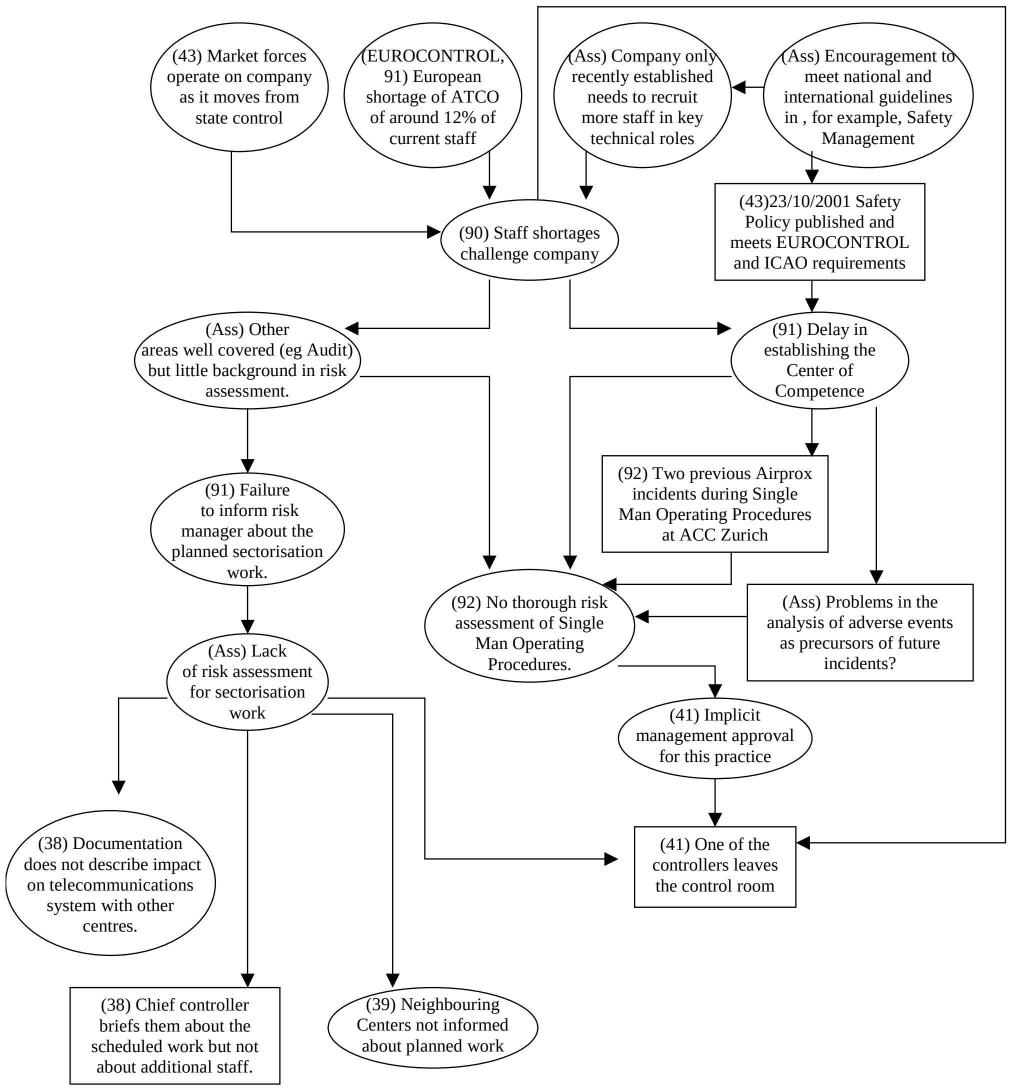

Figure 1: Interaction between Safety Management System and Lead-Up to the Accident

THE ORGANISATIONAL CONTEXT IN ACC ZURICH

Figure 2 starts with the observation that ACC Zurich upper airspace was divided both vertically and horizontally. The particular vertical division about FL235 into 2 or 3 sector operations created particular problems for the introduction of Revised Vertical Separation Minimum (RVSM). Switzerland was one of forty one European and North African countries that introduced a revised minimum separation of 300m (1000ft) between aircraft on 24 January 2002. This provided six additional cruising levels between FL 290 and FL 410 and was intended to reduce both fuel costs and delays. As part of their preparations for the introduction of RVSM, Zurich Air Traffic Control Center developed a six hour project to modify the flight plan processing system to simplify the upper airspace. This effected a number of different systems: the ADAPT radar data application; the multi-radar computer system; the flight plan data processing system for tower and approach control; the landing sequence computer; the departures and arrivals traffic management system and the ground to ground phone system with neighboring centers. Figure 1 also shows how management began to prepare for the upgrade by issuing official instructions Z-2002-022 and 024. These outlined the proposed work and an additional memorandum documented the impact that it would have for controllers. In particular, they would have to operate without all of the functionality that was normally provided by their Short-Term Conflict Alert (STCA) system.

The right-half of Figure 2 builds on the previous organizational analysis of Skyguide. In particular, it links problems in safety management to the lack of effective risk assessment for the particular work that was proposed within the Zurich ACC. The evidence for problems in safety culture is provided on page 91 of the BFU report. However, the official investigation does not explicitly consider whether or not a more sustained risk assessment would have identified the potential hazards. In consequence, the associated contributory factors in Figure 2 are annotated shown as assumptions. The key point is that the ECF analysis helps to identify an apparent explanation, such as the lack of any adequate risk assessment, for the failure to document the impact of the upgrade on the telecommunications facilities with neighboring centers. Similarly, this failure can be used to explain the lack of documentation about the impact on night shift operations and the need to manually correlate radar targets against flight plan information.

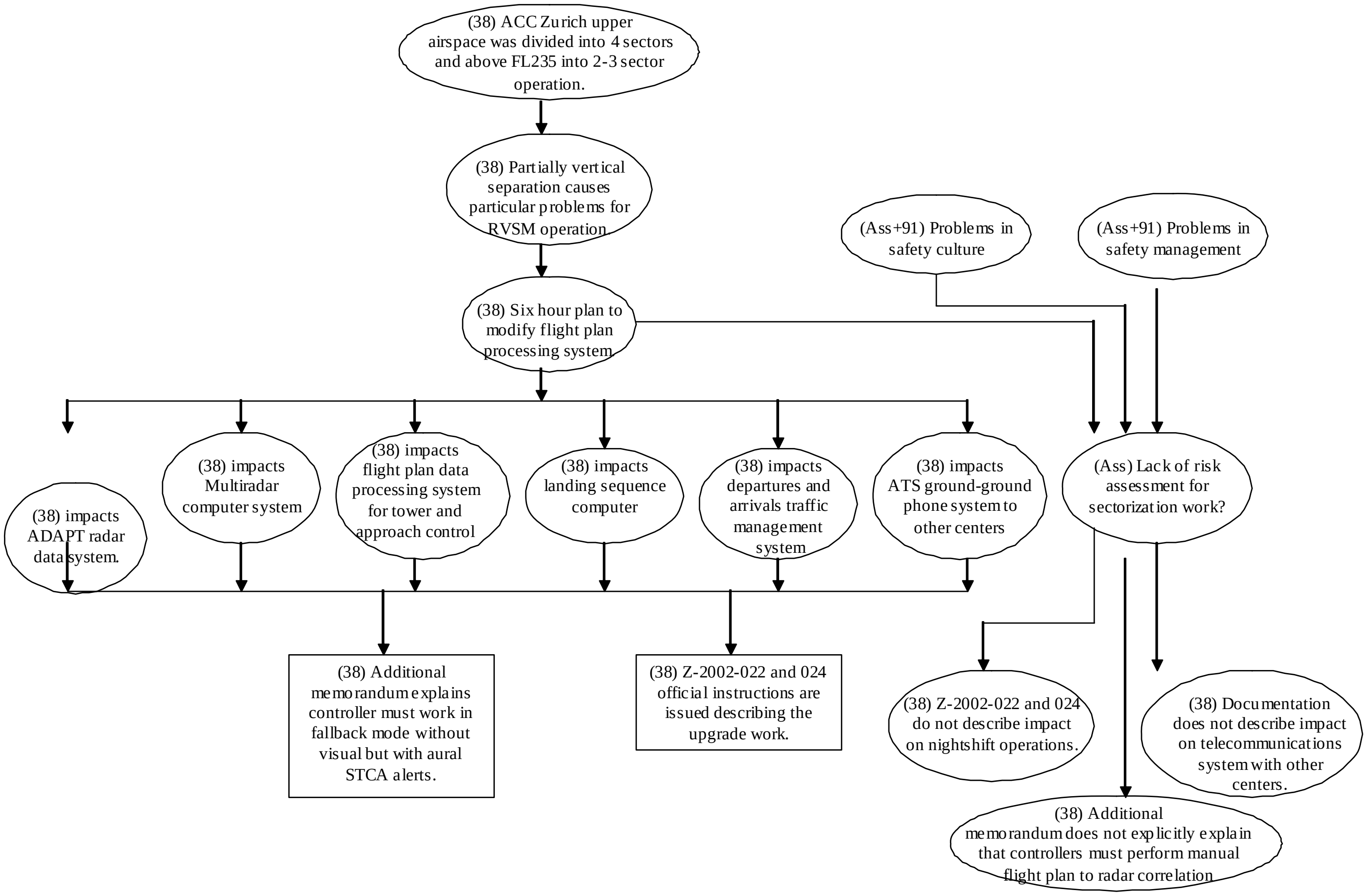

Figure 2: Contextual Factors Influencing the Technical Systems Environment in the Zurich ACC

HUMAN RESOURCES IN ACC ZURICH

Figure 3 focuses on human resource issues within ACC Zurich prior to the accident. The normal configuration was for two controllers to be supported by two assistants. It was also usual for one of the controllers to leave the control room as soon as traffic died down so that he or she could rest in the lounge. During the accident, one of the controllers left the control room. Management knew about this practice and there was no apparent pressure to stop it hence there was at least implicit acceptance, documented on page 41 of the BFU report. This may itself also be due to problems in safety-culture mentioned in the previous paragraphs [5]. The additional controller was now out of earshot from their colleague and the remaining controller believed they only had one assistant to call on for help.

Meanwhile, the six hour upgrade plan was also having an impact on the personnel and staffing of ACC Zurich, just as it had effected the technical environment. In this case, there was a systems manager (SYMA) who was available for support duties during the upgrade. However, they stayed at their workstation. Controllers were unaware that this resource was available. Under normal circumstances, the remaining controllers had to accept SYMA responsibilities after their shift ended around 21:00.

Similarly, there was an additional manager to coordinate work between the technicians and the controllers. The Chief controller briefed his two colleagues about the work at the start of the shift but did not tell them about the additional staff. In consequence, a single controller may have believed that they were responsible for the tasks associated with radar planning, radar execution, shift supervisor and systems manager at a time when profound changes were being made to the technical infrastructure.

The BFU argue that the safety culture and safety management practices of the ATM service provide should have ensured minimum manning levels. However, it can be argued that overstaffing of control room environments can lead to complacency, boredom and fatigue that are themselves error inducing factors during quiet intervals in safety-critical tasks. Hence, the ECF analysis in Figure 3 again reinforces the observation that it is not the under-manning itself that is the root cause of the problem. The accident was caused by a combination of the under-manning and a failure to recognize the risks associated with the profound system changes and lack of normal system support as a consequence of the SYCO flight plan processing system upgrade.

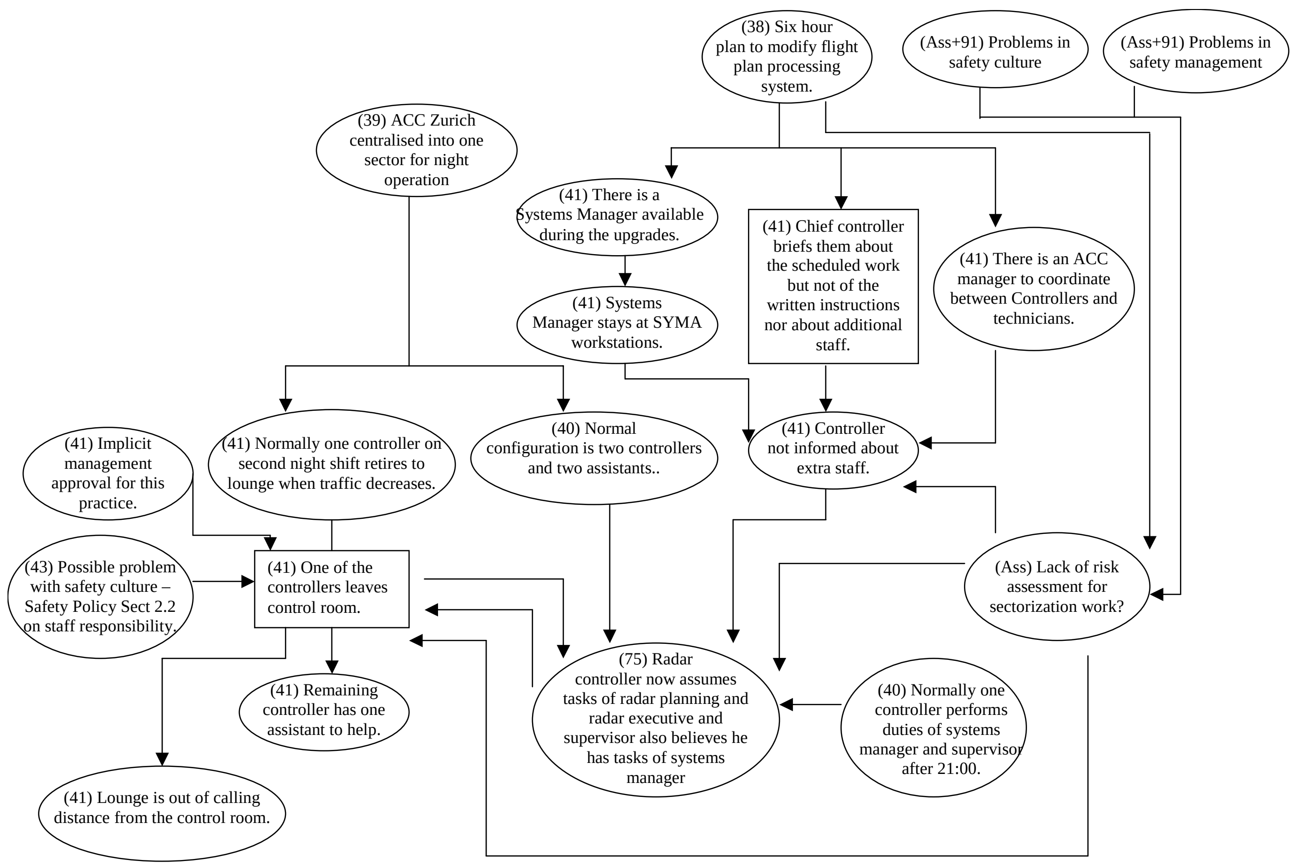

Figure 3: The Human Systems Environment in the Zurich ACC

The Radar Controller's Role in the Accident

Figure 4 takes the analysis from the time at which the controllers reported for duty (17:50). However, it also carries forward elements of the earlier analysis of the technical and personnel infrastructure. For instance, it refers to the lack of documentation on the impact of the upgrades. It also links back to the lack of any adequate risk assessment and the impact that this may have had on, for instance, the Chief Controller's briefing about the upgrade work. Similarly, this diagram includes elements of Figure 3 that refer to the remaining controller assuming a considerable number of additional responsibilities at a time when they were left exposed by a lack of systems support.

Figure 4 goes well beyond the previous ECF diagrams because it begins to map out the more immediate chain of events that led to the accident. As can be seen, the B757 contacts Zurich ACC at 21:21:50. The request is made for clearance to FL360 immediately after the initial contact and this is granted at 21:26:36. The conditions that make this event more likely include the fact that the paper control strips for the B757 and TU154M do not show any apparent conflict. They were cleared to different waypoints. The controller's difficulty in anticipating the potential conflict is compounded by the observation on page 75 of the BFU report that the strips no longer began to reflect the true situation as the TU154M was shown at FL350 after Trasadingen VOR. However, the controller would have had to detect this inconsistency manually given that the automatic flight plan and radar correlation (ADAPT) support had been disabled as part of the SYCO flight plan processing system upgrade. The ECF diagram ends with the call from the TU154M to Zurich ACC as it approaches their airspace.

The key insight from Figure 4 is the role that inadequate risk assessment may have played in exposing the Controller to an error inducing context. This builds on the previous contextual analysis that has already made a similar point because it shows the more detailed causal mechanisms that led from managerial and cultural problems to specific events in the accident itself. In this case, the lack of risk assessment led to the controllers being poorly informed about the sectorisation work. It is possible to conjecture that if additional information had been available, for instance about the interruption to the SWI-02 communications system with neighboring centers then the second controller might not have departed for the lounge. Similarly, if an adequate risk assessment had been conducted then additional consideration might have been paid to the possible consequences of disabling the ADAPT radar system.

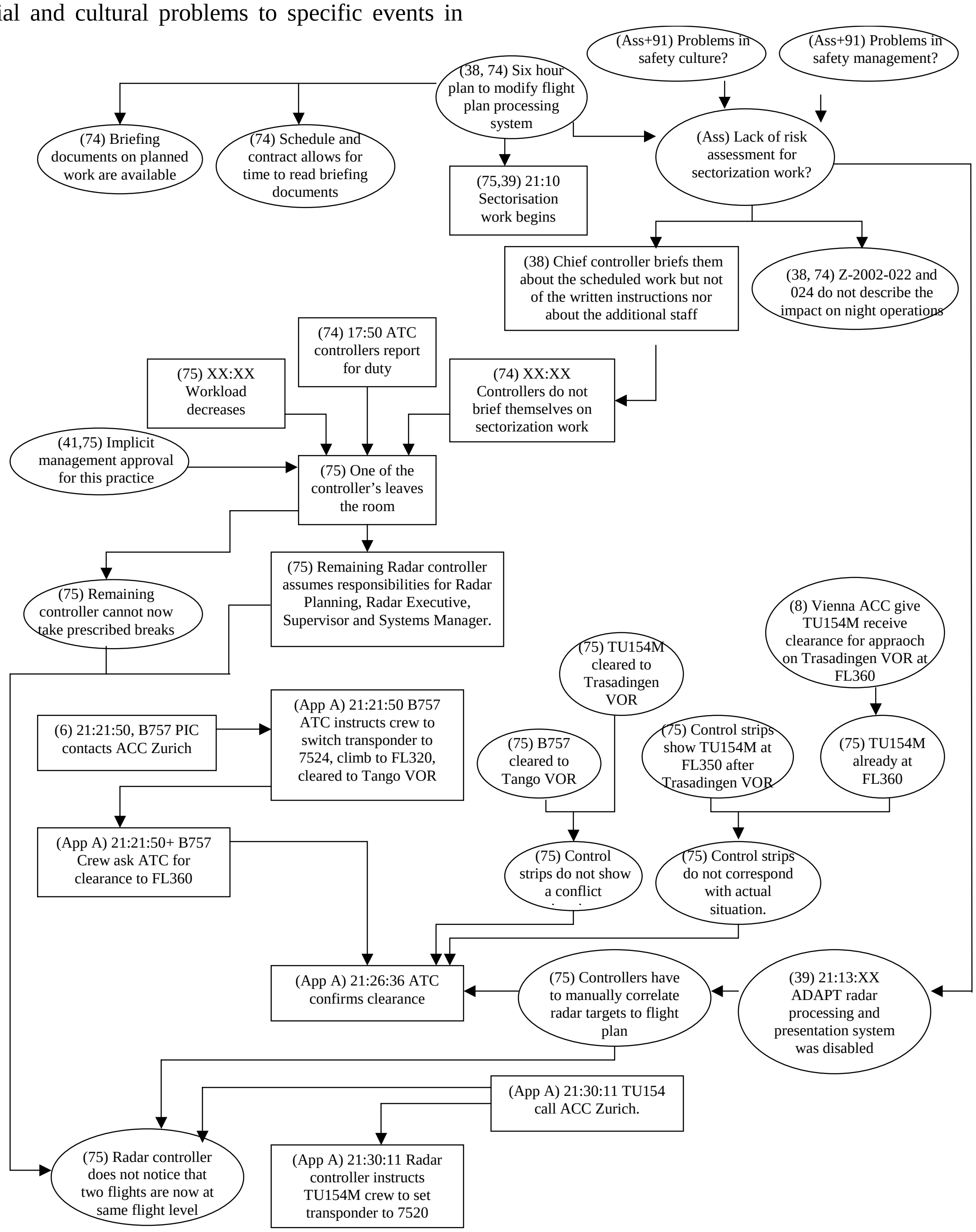

Figure 4: Clearance for B757 to Join TU154M at FL360

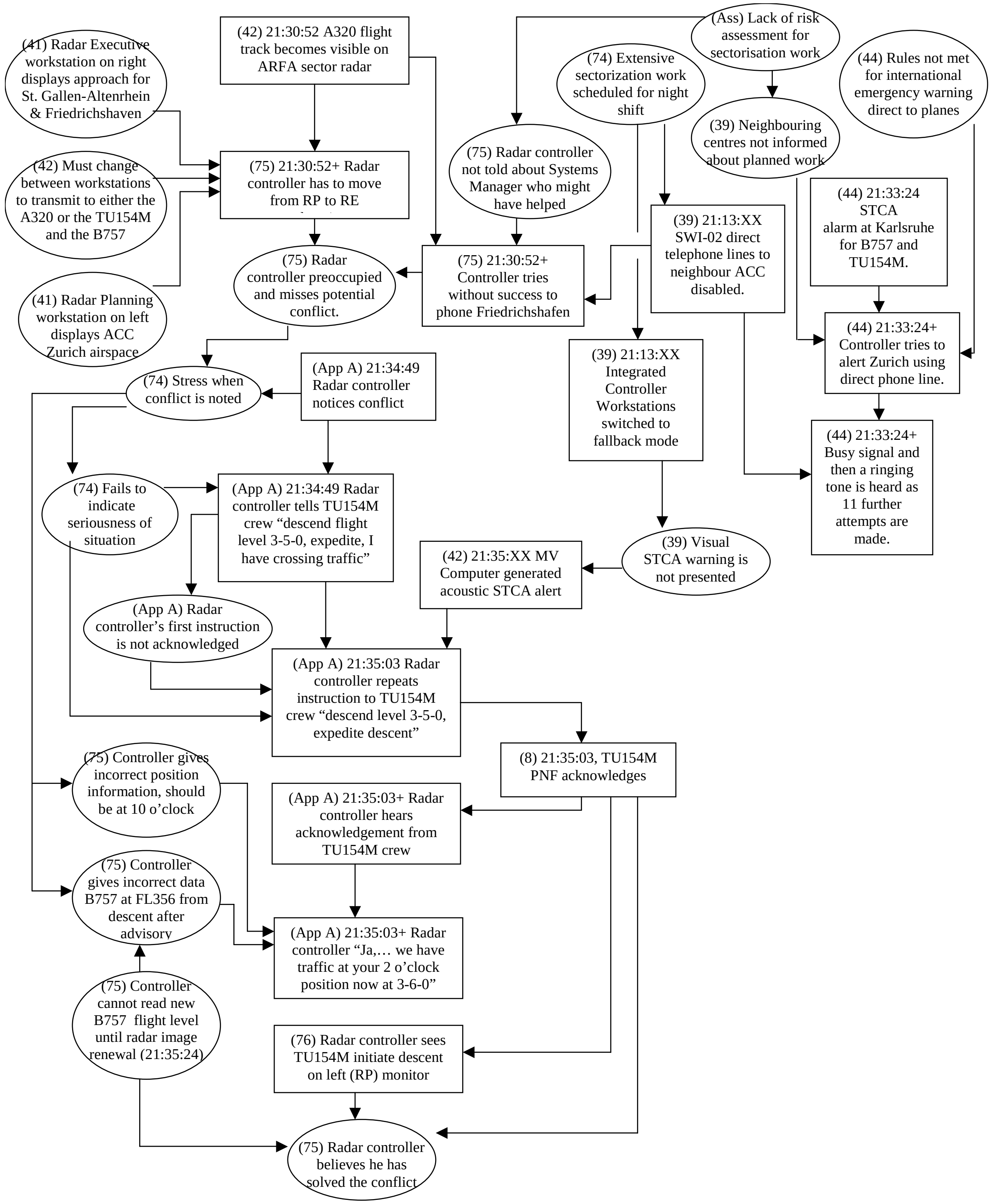

Figure 5: Radar Controller Notices and Attempts to Resolve Conflict

It is important to emphasize that the analysis of ECF diagrams relies upon counterfactual arguments. The previous paragraph surmises that the accident would not have progressed in the way that it did had an adequate risk assessment been performed. We cannot, however, be sure that this would indeed have been the case. We cannot run an experiment or realistic simulation to show that such an assessment would have uncovered the potential hazards that the controllers, aircrews and passengers faced during this accident. Equally, the ECF analysis does point the need to be more coherent about the particular safety management techniques that might have been used to detect the potential problems before lives were placed at risk. As we have seen, the BFU recommendations correctly focus on staffing issues and the performance of ACAS/TCAS. In addition, however, recommendations should be made about the role of specific and concrete safety management techniques that are consistent with a strong safety culture. The analysis in this report would, therefore, suggest that a risk assessment should have identified the potential dangers associated with the upgrade long before the two controllers set foot in the ACC Zurich.

Figure 5 continues the ECF analysis from the moment when the TU154M approaches ACC Zurich to the point at which the BFU argue the Controller believed he had resolved the conflict. Key observations in this stage of the analysis are that at 21:33:24 there is an Short Term Conflict Alert (STCA) at Karlsruhe. This is one minute and eighteen seconds before the TCAS warning on the aircraft and approximately two minutes between the missed audible STCA warnings at ACC Zurich. During this interval it might have been possible for the Karlsruhe staff to alert the controller to the potential problem, however the SWI-02 direct communications facility had been interrupted as part of the upgrade work. Similarly, the visual STCA warning at ACC Zurich was also disabled. This might have bought an additional two minutes warning compared to the time at which the controller began responding to the conflict.

Figure 5 illustrates another possible reason for the controller's failure to detect the potential conflict. An A320 flight entered the controller's area and he attempts to coordinate with Friedrichshaven. As we have seen, neither the controller nor the neighboring areas were informed of the potential interruption to the SWI-02 communications system. Valuable time was lost as the controller distributed his finite attention between the three aircraft and the associated tasks. The demands associated with these tasks were exacerbated by the layout of the controller's working positions. He had to shuffle between two workstations; both were capable of displaying the flight radar information but different positions had to be used to broadcast to the TU-154M and the B757 on one frequency and the A320 on another. All of these factors may have combined with the lack of an automatic radar and flight plan correlation system to prevent the controller form recognizing the conflict. Figure 5 captures the extreme situation that faced the controller. The BFU report argues that these problems could have been resolved by adequate staffing. Equally, however, a more coherent risk assessment strategy should also have uncovered the need to fully document the consequences of the upgrade. It also may have emphasized the importance of communicating those consequences both to controllers and to other centres. Although the BFU mention the importance of information dissemination in recommendation 01/2003, it does not link the recommendation to any of the immediate or systemic causes of the accident. In contrast, Figure 5 shows how this recommendation can be more directly tied into the events leading to the Überlingen accident. In particular, the lack of an adequate risk assessment can be argued to have created the context in which the accident occurred.

Figure 5 shows that the controller notices the conflict between the B757 and TU154M at 21:34:49. It is difficult to determine the precise cognitive and perceptual factors that prompted his subsequent intervention. The diagram does, however, introduce an assumption that the stress of detecting a potential conflict under such adverse working conditions may explain his apparent failure to inform the aircrews of the seriousness of the incident, noted on page 74 of the BFU report. The ECF diagram denotes that the initial descend command was not explicitly acknowledged by the TU154M crew and so the instruction is reiterated. The Pilot-Non-Flying acknowledges the second request and the controller responds by, arguably, explaining the request; 'Ja,… we have traffic at your 2 o'clock position now at 3-6-0'. Again the stress of the situation may explain the apparent anomaly in this comment when the B757 should have been in the 10 o'clock position relative to the TU154M. At this point the controller observes the descent of the TU154M as requested but cannot observe the descent of the B757 in response to their TCAS advisory because the controller's radar image is not renewed until 21:35:24. Hence, the BFU argue that he believed he had resolved the conflict.

Figure 6 illustrates the immediate events before the collision. Again, the controller begins to focus his attention on the A320 on its delayed approach to Friedrichshafen. This allocation of attention is explained in the BFU report by the observation that the Controller now believed they had resolved the conflict once the crew of the TU154M had expedited their descent to FL350. The decision to focus on the A320 had important consequences as the controller again had to move to the Radar Executive workstation to transmit to this aircraft. Any subsequent transmissions to the B757 or the TU154M would then involve a move back to the Radar Planning workstation, although all flights were visible on both displays. The outcome of this 'distraction' or division of attention was that the controller failed to observe the radar trace of the B757's descent in response to the previous TCAS advisory.

The controller's preoccupation with the A320 and the split working positions may also explain his failure to notice the B757 crews' radio signal to warn of a 'TCAS descent'. The BFU report suggests that the timing of this call was particularly unfortunate. The crew of the B757 had been trained to alert ATC as soon as possible after a TCAS advisory. Both the Pilot Flying and the Pilot Not Flying initially tried to contact ACC Zurich. It seems that the Controller's descent instructions to the TU154M and the subsequent conversation about the possible '2 o'clock' position of the other aircraft prevented the B757 crew from conveying the critical information about their decent to ACC Zurich:

> "Although the "TCAS descent" call was made 23 seconds after the beginning of the initial RA, and 7 seconds or more after the copilot was back on headset, it was made at the earliest opportunity. Immediately after the RA the Commander was PF and PNF, and was concentrating on the manual flying task to execute the RA manoeuvre, so that at that time the report of the "TCAS descent" did not have the highest priority. A few seconds after the RA the ATC frequency became busy with communication between Zurich Control and TU154M. The B757-200 crew

started their "TCAS descent" call as soon as the frequency became open". (BFU, page 94)

When the radio channel eventually became available, the B757 crew transmitted their descent call. However, this in turn overlapped with the call from the A320 crew on their approach to Freidrichshaven. This pathological sequence of events may, therefore, have prevented the controller from hearing the critical information from the B757 crew. Although, it can also be argued that when this information was transmitted there was insufficient time available to successfully avert the collision. Thirteen seconds provides an extremely narrow window within which to formulate a response, communicate that advice to one of the crews and for them then to act upon that information especially given that both crews had already initiated a decent to resolve the apparent conflict.

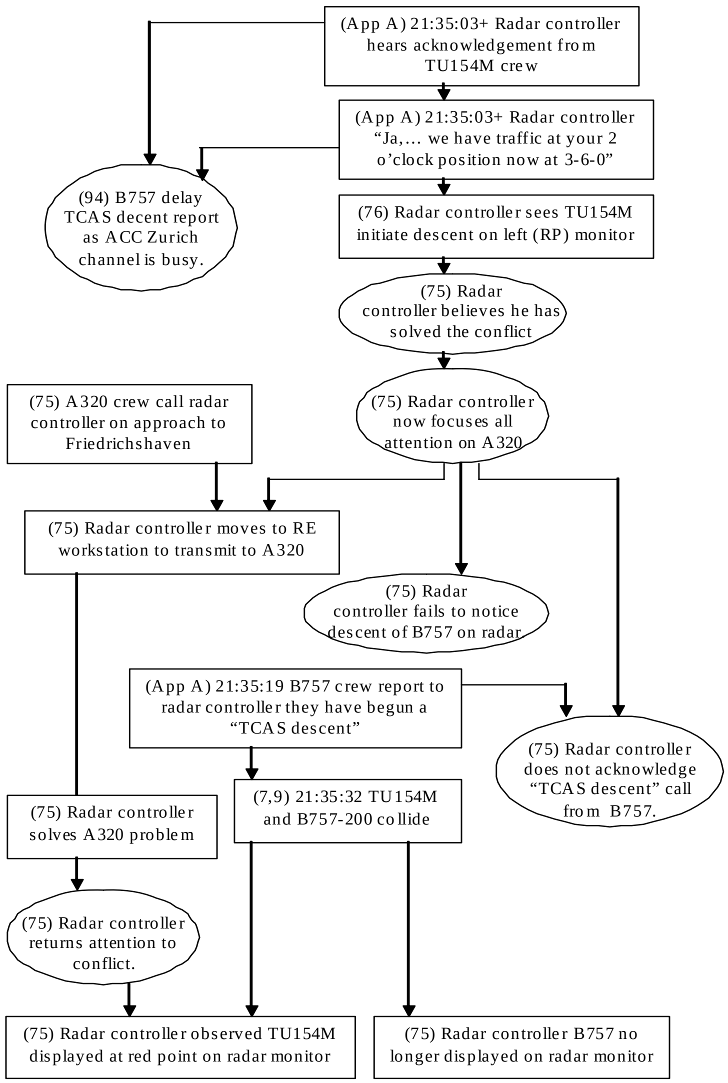

Figure 6: B757 TCAS Descent

CONCLUSION

This paper has focused on the role that Air Traffic Management played in the causes of the Überlingen mid-air collision. Most previous attention has been focused on the role of TCAS and on the manning of Zurich ACC. In contrast, we have focused on the wider lessons that can be learned from this accident. Events and Causal Factor models have been used to map out the interaction between technical, human factors and managerial causes. We have shown how problems in safety management helped to create an error inducing context. The lack of any sustained risk assessment created a situation in which controllers lost key elements of their technical infrastructure, including the SYCO flight processing system and the telecommunication infrastructure with neighboring centers. Our analysis also points to the dangers that arise from a 'can do' attitude in which staff use a wide range of 'work arounds' when faced with a degraded technical infrastructure. Controllers were willing to manually correlate targets and flight plans without the flight processing system. Other workarounds included the way in which ATCOs would shuffle between workstations in order to multiplex radio frequencies. They also include the various strategies that the controller employed as he tried to contact Friedrichshaven in the moments before the accident.

This analysis has strong parallels with the causes of the Linate runway incursion described in a companion paper also submitted to this conference. At Überlingen, the ACC Zurich staff faced relatively short-term changes in their infrastructure as the upgrade operations begain. In contrast, the Linate ATCOs faced a more gradual degradation in their technical environment as ground movement radar upgrades were successively delayed and official documentation no longer reflected the taxiway markings that were visible to aircrews. In both accidents, managerial and organizational factors created the context in which operators were likely to make mistakes. However, both accidents illustrate the remarkable lengths that ATCOs will go to in order to maintain air traffic services. This continues to be a significant concern even for those Air Navigation Service Providers that have a relatively good safety record. It is relatively easy to find the post-it notes, upgrade requests and operational updates, which document the daily 'work arounds' that help to maintain air traffic services in many operational centers.

ACKNOWLEDGMENTS

Thanks are due to Gilles le Galo and Tony Licu for providing constructive feedback about early versions of this paper.

REFERENCES

1. Bundesstelle für Flugunfalluntersuchung (BFU: German Federal Bureau of Aircraft Accidents Investigation), Accident on 1 July 2002, Near Überlingen/Lake Constance, Germany Involving Boeing B757-200 and Tupolev TU154M, Investigation Report AX001-1-2/02, May 2004.
2. C.W. Johnson, A Handbook of Accident and Incident Reporting, Glasgow University Press, Glasgow, 2003.
3. NASA, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping, NPR: 8621.1A, Code Q/Office of Safety and Mission Assurance, Washington DC. 2004.
4. 2. D. Woods and R.I. Cook, The New Look at Error, Safety, and Failure: A primer, Technical Report, US Veterans Association, National Centre for Patient Safety, 2004.
5. D. Wiegmann and S.A. Shappell, A Human Error Approach to Aviation Accident Analysis, Ashgate Publishing, 2003.