Final Report:

Review of the BFU Überlingen Accident Report

(Version 1: 17/12/2004)

Contract C/1.369/HQ/SS/04

Overview of the Project

This project reviews the BFU report into the Überlingen Accident. The analysis concentrates on the BFU report and investigation. However, additional references are made to EUROCONTROL and other external recommendations, especially in the area of safety Management Systems. The aims of this work are to: 1. to show how the existing recommendations relate to the root causes identified in the existing report. 2. to use recognised accident analysis techniques to identify additional recommendations that might be derived from this accident. 3. to review the existing BFU report and the Swiss government investigation into the associated safety management systems to extend the scope of objective (2).

Executive Summary of the Final Report

Technical Report A: The existing BFU report focuses on issues surrounding the coordination of aircrew responses to TCAS advisories in the face of possibly conflicting instructions from Air Traffic Service personnel. It also provides a thorough account of safety management issues surrounding the staffing and operation of the Zurich ACC during major maintenance and upgrade operations. In contrast, the analysis in this report looks beyond the operating environment in the Zurich control room on the night of the accident. Greater emphasis is placed on adequate preparation for what was extensive technical procedures that deprived the controllers of necessary support and created an 'error inducing' environment. In particular, the BFU report provides few insights into the risk assessment procedures that should be used before any similar upgrades should be attempted in the future.

Technical Report B: This second part of this document builds on the findings mentioned above. In particular, it goes on to look at the role that Safety Management Systems played in the accident. We concur with the BFU that the Swiss authorities had well-documented procedures and principles that would encourage the development of a sound Safety Management System. These principles were in accordance with ICAO and EUROCONTROL guidelines. However, the Swiss ATM organisations lacked the experience and the personnel to implement those procedures. Partly as a result of this opportunities were missed to learn from two AIRPROX incidents that had similarities to the events before the Überlingen accident. A number of additional recommendations are presented in this report that build on those recommendations already provided in Technical Report A. The report closes by analysing the insights that the accident provides for the recent guidance published on Safety Management Systems in ATM operations by EUROCONTROL, Transport Canada and the US FAA.

Prepared by:

Prof. Chris Johnson
217, Wilton Street, North Kelvinside, Glasgow, G20 6DE, Scotland, UK.
Johnson@dcs.gla.ac.uk (Email), +44 141 330 6053 (Tel.), +44 141 330 4913 (Fax)

Technical Report A:

Incorporating Deliverables 1 and 2

(Version 1: 15/12/2004)

Contract C/1.369/HQ/SS/04

Executive Summary of Technical Report A

The following pages provide the first deliverable from this project. They document the output from an initial analysis of the BFU report. The investigation began by first constructing a more detailed timeline of the events leading to the collision, from the perspective of both crews and the Radar Controller who was operating the position in Zurich ACC. This involved the compilation of additional details beyond the high-level summary that is provided in Appendix 2 of the BFU report. Once this timeline had been compiled, it was used to generate more complex Events and Causal Factors charts. These focussed on the influences that helped to shape the controllers interaction with the aircrews and with neighbouring centres during the crucial minutes before the collision. Our analysis identified a number of minor ambiguities and inconsistencies in the English language version of the report. It also extended the scope of the BFU investigation. The existing report focuses on issues surrounding the coordination of aircrew responses to TCAS advisories in the face of possibly conflicting instructions from Air Traffic Service personnel. It also provides a thorough account of safety management issues surrounding the staffing and operation of the Zurich center during major maintenance and upgrade operations. In contrast, the analysis in this report looks beyond the operating environment in the Zurich control room on the night of the accident. Greater emphasis is placed on adequate preparation for what was extensive technical procedures that deprived the controllers of necessary support and created an 'error inducing' environment. In particular, the BFU report provides few insights into the risk assessment procedures that should be used before any similar upgrades should be attempted in the future.

Prepared by:

Prof. Chris Johnson
217, Wilton Street, North Kelvinside, Glasgow, G20 6DE, Scotland, UK.
Johnson@dcs.gla.ac.uk (Email), +44 141 330 6053 (Tel.), +44 141 330 4913 (Fax)

Introduction

In the EUROCONTROL Strategic Safety Action Plan (SSAP) framework, informal and more formal reviews of the BFU Überlingen Accident Report have been carried out in order to identify safety improvement that might not have emerged from the initial investigation. So far, few additional recommendations have been identified. This report, therefore, represents the first set of deliverables from a detailed review of the BFU report by an independent team of accident investigators. The key objectives for this study are:

1. to show how existing recommendations relate to root causes identified in the existing report. The main focus will be to use Events and Causal Factors diagrams to draw out the root causes from the report and then to relate them to the recommendations. This choice of this method is justified because it provides relatively accessible diagrams that can readily be inspected to trace the information in the report back to particular recommendations. EUROCONTROL has used similar diagrams to model human error and systems failure in ATM incidents, for example in HUM.ET1.ST13.3000-REP-02 Human Factors in the Investigation of Accidents and Incidents.

2. *to use recognised accident analysis techniques to identify further recommendations from this accident.* The ECF model developed in the previous stage of analysis can also be used to help identify additional recommendations. This will be done using the associated reasoning techniques that are part of this method. Additional root causes can be identified by examining each element of the diagram and asking whether or not the accident could have been avoided if that event had not occurred. If the answer is yes then the event or condition becomes a candidate for further inspection.

3. *to review the existing BFU report and other reports into this accident dealing with the associated safety management systems to extend the scope of objective (2).* This final stage of the project will look more closely at the findings from the second stage of analysis. Rather than focussing on the BFU report alone, this stage will look at the wider investigatory process in the context of SMS development and will refer to investigatory practices in other countries. In particular, comparisons will be drawn with the FAA and Canadian TSB's guidelines on SMS development.

There are three deliverables associated with this project. Each represents the output of one of the stages identified in the previous section. The first is to deliver an analysis of the mapping from recommendations to root causes in the BFU report. The second is to identify appropriate additional recommendations. The final deliverable is a report documenting each of the previous two subtasks and linking the information described in (1 and 2) to associated work on safety management system guidance within ATM. As mentioned, this document provides the first two of these three deliverables.

The BFU report into the Überlingen collision identified a number of immediate causes for the accident. These can be summarised as follows, all page numbers in the remainder of this report refer to the official BFU English language translation of the original German report:

• (Immediate Cause 1) "The imminent separation infringement was not noticed by ATC in time. The instruction for the TU154M to descend was given at a time when the prescribed separation to the B757-200 could not be ensured anymore". (BFU page 112)

• (Immediate Cause 2) "The TU154M crew followed the ATC instruction to descend and continued to do so even after TCAS advised them to climb. This manoeuvre was performed contrary to the generated TCAS RA". (BFU page 112)

In addition, the BFU also identified a number of less immediate systemic causes:

• (Systemic Cause 1) "The integration of ACAS/TCAS II into the system aviation was insufficient and did not correspond in all points with the system philosophy. The regulations concerning ACAS/TCAS published by ICAO and as a result the regulations of national aviation authorities, operational and procedural instructions of the TCAS manufacturer and the operators were not standardised, incomplete and partially contradictory". (BFU, page 112)

• (Systemic Cause 2) "Management and quality assurance of the air navigation service company did not ensure that during the night all open workstations were continuously staffed by controllers". (BFU, page 112)

• (Systemic Cause 3) "Management and quality assurance of the air navigation service company tolerated for years that during times of low traffic flow at night only one controller worked and the other one retired to rest." (BFU, page 112)

The first stage of our analysis was intended to determine the relationship between this causal analysis and the 19 recommendations that were presented in the BFU report. Table 1 provides an overview of the results from an initial analysis. It also documents the organisations that each recommendation was directed at. Most of the recommendations are directly related to the immediate and systemic causes identified in the BFU report. For instance, the recommendation 18/2002 made to the ICAO on 1st October 2002 relates to changes in the requirements of Annex 2 and 6 and the PANS-OPS documentation to ensure that pilots follow TCAS advisories even in the face of conflicting information from ATM officers. This clearly addresses immediate cause 2 in which the crew of the TU154M descended 'contrary to the TCAS RA'. It can also be argued that this recommendation stems from systemic cause 1 that the 'integration of ACAS/TCASII into the system aviation was insufficient'.

Similarly, from an ATM perspective recommendation 02/2003 issued on the 21st July 2003 required the Swiss Federal Office for Civil Administration ensure minimum staffing levels at Zurich ACC. This addressed immediate cause 1, that the 'separation infringement was not noticed by ATC in time'. It also addressed systemic cause 2, the 'management and quality assurance of the air navigation service company did not ensure that during the night all open workstations were continuously staffed by controllers'. Finally, this recommendation also addresses systemic cause 3 identified in the BFU report, the management and quality assurance programmes 'tolerate for years that during times of low traffic at night only one controller worked and the other retired to rest'.

However, several of the recommendations do not relate directly to either the immediate or systemic causes identified in the BFU report. This can be explained in a number of ways. For instance, Recommendation 09/2004 focuses on the need to improve audio recording of a controller's workstation to support accident investigation. Similarly, 13/2004 urges the Swiss Federal Office for Civil Aviation to meet the EUROCONTROL recommendations for data capture and the reconstruction or replay of adverse events and near miss incidents. Such recommendations cannot be directly related to the causes of the accident but are formed in response to problems during the investigation itself.

Reference and Date	Recommendation To	Summary of Recommendation	Cause Addressed?
18/2002 (1st Oct. 2002)	ICAO	Changes to Annex 2 and 6 and PANS-OPS to require pilots to follow TCAS advisories.	Immediate 2, Systemic 1
01/2003 (21 July 2003)	Swiss Federal Office for Civil Aviation	Dissemination of information about and planning of maintenance work on ATC system (NB, no explicit mention of risk assessment)	
02/2003 (21 July 2003)	Swiss Federal Office for Civil Aviation	Ensure minimum manning levels in ACC Zurich	Immediate 1, Systemic 2, Systemic 3
03/2003 (21 July 2003)	Swiss Federal Office for Civil Aviation	ATC personnel to be trained in theory and simulation of emergency procedures.	Immediate 1, Systemic 3
06/2004 (19 May 2004)	ICAO	Annex 2, 6, PANS clarification of pilots responses to ACAS resolution advisories (RAs).	Immediate 2, Systemic 1
07/2004 (19 May 2004)	ICAO	Improve pilot education and training to increase confidence in ACAS.	Immediate 2, Systemic 1
08/2004 (19 May 2004)	ICAO	Downlink RA's to ATC.	Immediate 1
09/2004 (19 May 2004)	ICAO	Assist accident investigation by recording speech and noise etc at ATC workstations similar to cockpit voice recorders.	
16/2004 (19 May 2004)	ICAO	Ensure all ACAS/TCAS users should be consistent in responses to devices.	Immediate 2, Systemic 1
10/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Minimum requirements for provision of Short Term Conflict Alert to all ATC units.	Immediate 1
11/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Provide backup telecommunications systems in case of failure of main system.	
12/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Radar updates within 8 seconds or less in en-route air space.	Immediate 1
13/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Meet EUROCONTROL recommendations for surveillance and data capture so it is possible to reconstruct critical incidents.	
17/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Meet ICAO SARPS and EUROCONTROLS ESARRs for Safety Management Systems (NB, no explicit mention of risk assessment).	Systemic 2
18/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Require evaluation of minimum staffing levels.	Immediate 1, Systemic 2, Systemic 3
19/2004 (19 May 2004)	Swiss Federal Office for Civil Aviation	Refresher and safety training requirements compliant with ESARR 5.	Immediate 1
14/2004 (19 May 2004)	CAA of the Russian Federation	ACAS training to include simulation, CRM and LOFT programmes to include ACAS scenarios.	Immediate 2, Systemic 1
21/2004 (19 May 2004)	CAA of the Russian Federation	Advance the use of CRM training.	Immediate 2
15/2004 (19 May 2004)	US Federal Aviation Administration	Manufacturer rephrase TCAS 2000 manual to reflect international policy.	Systemic 1

Table 1: Summary of Recommendations Made in the BFU Report (pages 111-113)

Table 1 shows that the BFU have responded well in drafting recommendations that address each of the immediate and systemic causes they identified for the accident. Previous paragraphs have argued that most of the BFU recommendations are well justified in terms of the immediate and systemic causes that are identified in the report. Some of the other recommendations cannot be related back to the causes of the accident because they address problems in the investigation rather than the events that led to the mishap. In contrast, a number of recommendations cannot be linked directly to the causes identified in the BFU report. This raises a number of issues. For example, it might be argued that these recommendations are poorly grounded in the evidence that was gathered in the aftermath of the accident. Alternatively, these recommendations might address important safety issues for which there had only been a partial causal analysis. In other words, interventions were recommended without identifying the associated immediate or systemic causes. These recommendations include 01/2003 looking at the

dissemination of information about the planning and maintenance work on ATC systems. They also include recommendation 11/2004 on the need to provide backup telecommunications systems in the event of a main telecommunications system failure.

The following pages further analyse the evidence that supports these recommendations (01/2003 and 11/2004) that appear unrelated to the immediate and systemic causes. The analysis also determines whether any additional recommendations might be drawn from the BFU report into the Überlingen accident. In order to do this it is first necessary to develop a more detailed timeline of the events that led to the mid-air collision.

The Detailed Timeline

Appendix 2 of the Überlingen report contains a high level timeline of the events that led to the collision. This sequence of events runs from 21:21:50 until 21:35:32. The timeline provides an excellent overview of the accident. It describes communications between the ACC and the crew of both the B757 and the T154M. It also describes some of the actions that were taken in the immediate run-up to the collision. For example, it includes information about the separation and altitude of each aircraft at key moments. As far as is possible, each event is associated both with the real time at which the event occurred and the elapsed time until collision. Table 2 provides an excerpt from Appendix 2 of BFU report.

Zeit UTC	Min Sek	Boeing B757-200 Flug DHX 611	Tupolew TU154M Flug BTC 2937
21:21:50	13:42	Initial call to ACC Zurich on 128.050 MHz at FL 260. The crew is instructed to switch the transponder to 7524, to climb to FL 320 and is cleared direct to Tango VOR. The crew requests a climb to FL 360. ACC Zurich announces the clearance in 4 to 5 minutes later.	
21:26:36	8:56	The crew receives the instruction to climb to FL 360.	
21:29:50	5:42	The aircraft reaches FL 360.	
21:30:11	5:21		Initial call to ACC Zurich on 128.050 MHz at flight level FL 360. The crew is instructed to witch the transponder to 7520.
21:33:03	2:29		Start of a conversation within the cockpit about a TCAS indication, which shows another aircraft in the same altitude.
…	…	…	…

Table 2: Except from Appendix 2 'Events in Both Cockpits' of the BFU report (Page 1 of Appendix file)

There are several important limitations that affect the BFU timeline. Firstly, it does not cover many of the contributory events that created the context in which the accident occurred. In particular, it does not mention any of the circumstances that relate to the two 'partially supported' recommendations identified in the previous section. Appendix 2 does not go back far enough to consider the dissemination of information about the planning and maintenance work on ATC systems (recommendation 01/2003) nor does it address the events that led to recommendation 11/2004 on the need to provide backup telecommunications systems in the event of a main telecommunications system failure. Secondly, the timelines in Appendix 2 is entitled 'Events in both Cockpits' hence the focus is not on the circumstances surrounding the controller's actions. It is for these reasons that our analysis began by reconstructing an extended and more detailed timeline of events. The reconstructed timeline was deliberately developed to consider the controller's perspective as well as the circumstances in both cockpits.

Appendix A of this report presents the extended timelines used in this initial stage of the analysis. In contrast, the remainder of this section goes on to review some of the key issues highlighted from this analysis. Firstly, the timeline was extended back to the moment at which both controllers came on duty (17:50). This is illustrated in Figure 1. In retrospect, this was not early enough. The subsequent Events and Causal Factors analysis of the two partially supported recommendations began to look at the management and planning of the SYCO flight plan processing system. For now it, however, it is sufficient to observe that this earlier start point was motivated by the aim of looking at the accident more from the perspective of Air Traffic Management staff rather than from the occupants of the two cockpits.

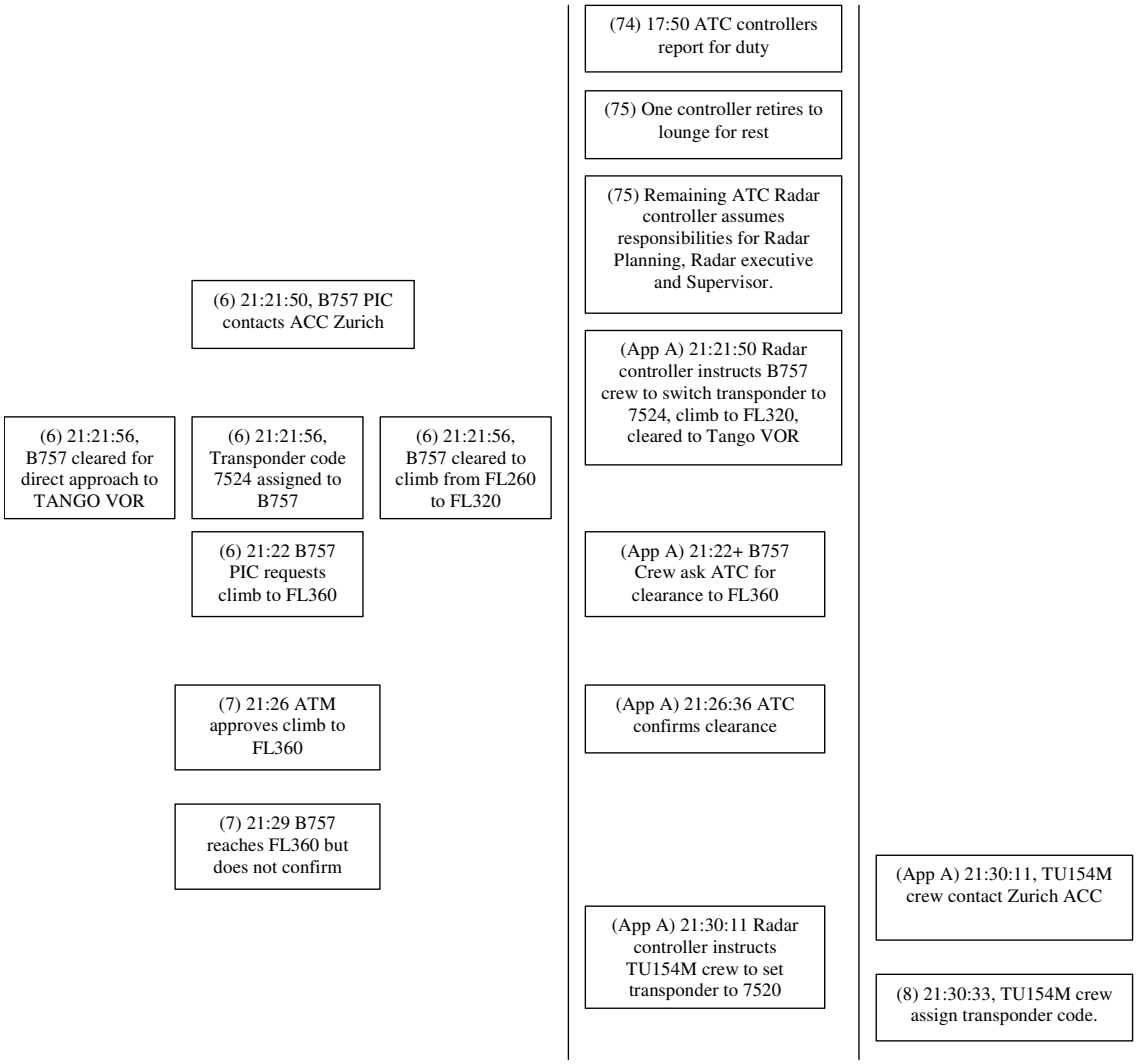

Figure 1: Except from the Revised Timeline of Events

In Figure 1, events are denoted by each rectangle. Time flows from the top to the bottom of the diagram. The left column is used to group events that relate to the B757. The middle column shows events associated with the Air Traffic Managers. The right column denotes events associated with the crew of the TU154M. The figures in brackets refer to pages in the BFU report that provide evidence for these events. For instance, "(8) 21:30:33 TU154M crew assigns transponder code" denotes that the BFU discusses the assignment of the transponder on page 8. A reference to "(App A)" relates to Appendix A of the BFU report.

Figure 1 illustrates some of the limitations of using timelines. For instance, this diagram denotes the B757 Pilot in Charge's request to climb to FL360. There is nothing here to indicate the implications or consequences of this request. The TU154M was already at FL360 and approaching the Zurich ACC centre. Nor does the timeline illustrate the factors that might have persuaded the controller to grant the request. As we shall see, paper based flight strips were used to replace some aspects of the SYCO flight plan processing system that was being upgraded and these paper strips did not show any potential conflict in the flight plans. The key point is that these timelines provide an entry point for any analysis and must be supplemented by additional techniques if they are to yield more detailed insights, for example about the partially supported recommendations that were identified in previous sections.

Having raised these caveats, it is important to stress that the process of developing these timelines can also help to identify potential conflicts, ambiguities and inconsistencies in accident reports. In particular, this analysis raised a

number of concerns about the precise time when the controllers might have been alerted to the audible STCA warning. On page 44 of the BFU report it is stated that:

> "At 21:35:00 hrs the MV computer of ACC Zurich generated an acoustic STCA message which was addressed to the workstation RE SUED. It was not heard by any of the staff members present in the control room" (BFU, page 44)

Page 77 extends this analysis by revealing that the several seconds before the STCA the controller was already aware of the potential conflict and was taking action, which he believed would resolve the situation. At 21:34:49 and again at 21:35:03 he issued instructions for the TU154M to expedite a descent. It is important to note that this excerpt does not mention the STCA audible alarm even though the controller's preoccupation with issuing descent instructions provide a cogent explanation for the failure to hear this alarm:

> "When the controller instructed the TU154M crew at 21:34:49 hrs for the first time to expedite descent to FL 350 the horizontal separation was practically already below 7 NM (exactly at 21:34:56, when the controller's radio message ended). The TU154M should have descended to FL 350 by 21:34:56 hrs to ensure a vertical separation of 1 000 ft in the RVSM airspace. To achieve this it would have been necessary to give the instruction to descend to FL 350 at 21:33:49 hrs at the latest - i.e. one minute before this instruction was actually given. This time is based on a normal rate of descent of approximately 1 000 ft per minute. When the TU154M crew did not verbally respond to the first instruction to descend to FL 350, the controller repeated this instruction at 21:35:03 hrs more emphatically". (BFU, page 77)

Again on page 91, a similar set of observations is made. The aural STCA alert was issued at 21:35:00, it was not heard by anyone. This paragraph does mention that the Controller had reacted to 'resolve the conflict' when the alarm was issued. It also stressed that by the time that the alert was issued the controller lacked both the information and time necessary to avert the collision:

> "The MV9800 computers released an aural STCA at 21:35:00 hrs, but this was not heard by anyone in the CIR. The aural alert was released 32 seconds before the collision. At the time the two aircraft had a distance of 6.5 NM to each other. As the ATCO had already reacted to resolve the conflict the aural STCA would just have pointed out the urgency of the situation. Even with the aural alert the ATCO would not have been able to recognize the situation was not evolving as he expected until further information was available. The TU154M was already complying with the descent instruction and the ATCO did not know the B757-200 had initiated an RA related descent. He would not have been able to recognise the B757-200 was descending until the screen update at 21:35:12 hrs or if he had heard the crew's TCAS descent call a few seconds later. By this time it was unlikely that he could have formulated an instruction that would have averted the collision with sufficient safety." (BFU, page 91)

The construction of the more detailed timeline helped to identify the importance of the STCA and the timing of the controller's initial response to the conflict. It raises a number of questions that are not fully analyzed in the BFU report. For instance, it is unclear when precisely the controller became aware of the potential conflict. Similarly, it is difficult to determine what might have made him aware of the potential conflict. For instance, Appendix 2 of the BFU report indicates that the TCAS alerts were generated in the two planes at 21:34:42. It does not record any communications that alerted the controller to the conflict and that might then have triggered his instruction to the TU154M to 'expedite' the descent at 21:34:49. It seems too much of a coincidence that the controller responded within seven seconds of the TCAS warning and so he may have been alerted by overhearing radio communications. However, this is not explicitly stated in the BFU report. If he had been alerted by other systems or observations then this might add further insight to the report.

Irrespective of the mechanisms by which the Controller was alerted to the conflict, our analysis has clearly shown the importance of the STCA system in this accident. The importance of this 'safety net' is not reflected in the existing BFU recommendations. The previous quote from paragraph 91 of the report clearly shows that even if the STCA warning had been heard and acted upon then it is unlikely that the collision would have been avoided. It should be recalled that Recommendations 07/2004, 16/2004, 14/2004 all deal with informing pilots about the operational strengths and weaknesses of TCAS/ACAS. Our analysis has shown that similar recommendations ought to be made so that controllers are aware of the role that STCA played in this accident. It is also important to emphasize the diverse ways in which the STCA was undermined by circumstance. An STCA alert was generated at the Karlsuhe center at 21:33:24 but could not be communicated because of problems with the SWI-02 telecommunications system. The visual STCA alert at ACC Zurich that would have been presented some two minutes before the aural alert was disabled as a result of the upgrade activities. One insight into the Überlingen collision is that current STCA systems provide a final safety net. They do not guarantee that controllers will be able to respond in time to avert an accident and hence, any use other than as a 'safety net' of last resort should be avoided.

Additional Recommendation 1:
Controllers should be made more aware of the role of STCA in the Überlingen accident as a reminder of the strengths and weaknesses of this tool. Our analysis and that of the BFU reinforces the role of STCA as a 'safety net' and not as an absolute defense against adverse events.

Background to the Upgrade of the SYCO Flight Plan Processing System

The initial analysis of the BFU report centred on the development a more detailed timeline that also considered the controller's perspective on the events leading to the collision. As mentioned, this analysis pushed back the initial timeline in Appendix 2 of the BFU report from 21:21:50 to 17:50 in the extended timelines of Appendix A in this report. However, subsequent analysis identified that the analysis would have to go further back to consider the events and conditions that created the context for this incident. In particular, such an extended analysis was necessary to consider the causal arguments that might back the recommendations that had not been fully supported in the BFU report; 01/2003 looking at the dissemination of information about the planning and maintenance work on ATC systems and recommendation 11/2004 on the need to provide backup telecommunications systems in the event of a main telecommunications system failure.

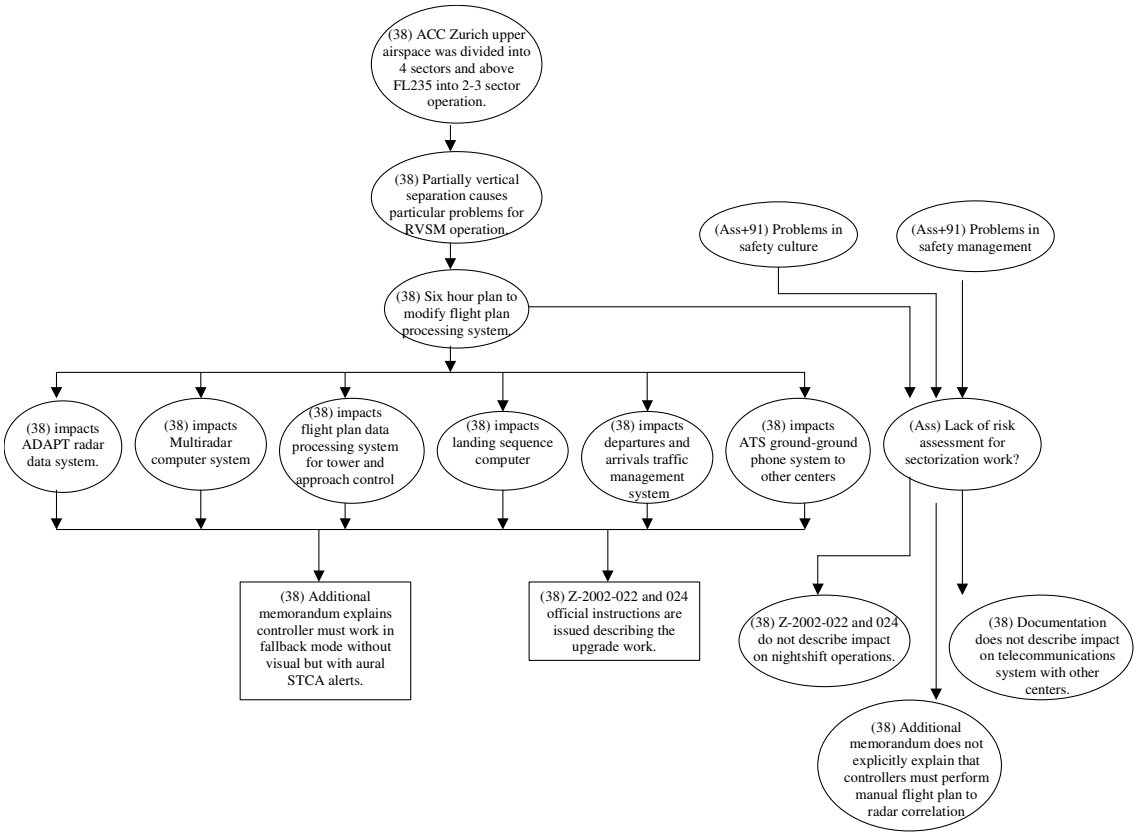

Figure 2: Contextual Factors Influencing the Technical Systems Environment in the Zurich ACC

Figure 2 presents the next stage in our analysis. It represents a simplified form of Events and Causal Factors analysis, initially pioneered by the US Department of Energy. Previous EUROCONTROL projects have used similar diagrams to model human error and systems failure in ATM incidents, for example in HUM.ET1.ST13.3000-REP-02 Human Factors in the Investigation of Accidents and Incidents. Ellipses are used to denote contributory factors that combine to make events more likely. Events, as before, are denoted by rectangles. The figures in parentheses refer to the page numbers in the BFU report that contain information about these contributory factors. This diagram sets the background for the more detailed causal modeling of the accident. As can be seen, Figure 1 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 operation created particular problems for the operation of RVSM and so page 38 of the BFU report outlines a six hour plan to modify the flight plan processing system to simplify the upper airspace and support the implementation of RVSM. This plan 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 ATS ground to ground phone system with neighboring centers. A further

consequence of these effects was that management began to prepare for the upgrade by issuing official instructions Z-2002-022 and 024 to describe the work. An additional memorandum also documented the impact that the work would have in requiring controllers to work in fallback mode without a visual STCA. The right-half of the diagram shows how ECF analysis can encourage investigators to look beyond the information that is presented in an official accident report. In particular, it denotes that problems in the safety culture and safety management may have prevented an effective risk assessment for the work that was to be undertaken. The evidence for problems in safety culture and safety management is provided on page 91 of the BFU report but it never explicitly considers the failure to perform a risk assessment, hence these contributory factors are annotated with 'Ass' for assumption. Technical report B will provide more detailed evidence from the BFU report and other sources to support this argument. The key point is, however, 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 other neighboring centers. Similarly, this failure can be used to explain the lack of documentation about the impact of the upgrade on night shift operations and on the need to perform manual correlations of radar targets against flight plan information.

Recommendation 2:
Additional emphasis should be paid to a risk-based approach to the identification and dissemination of information about the impact of necessary upgrades on the ATM infrastructure.

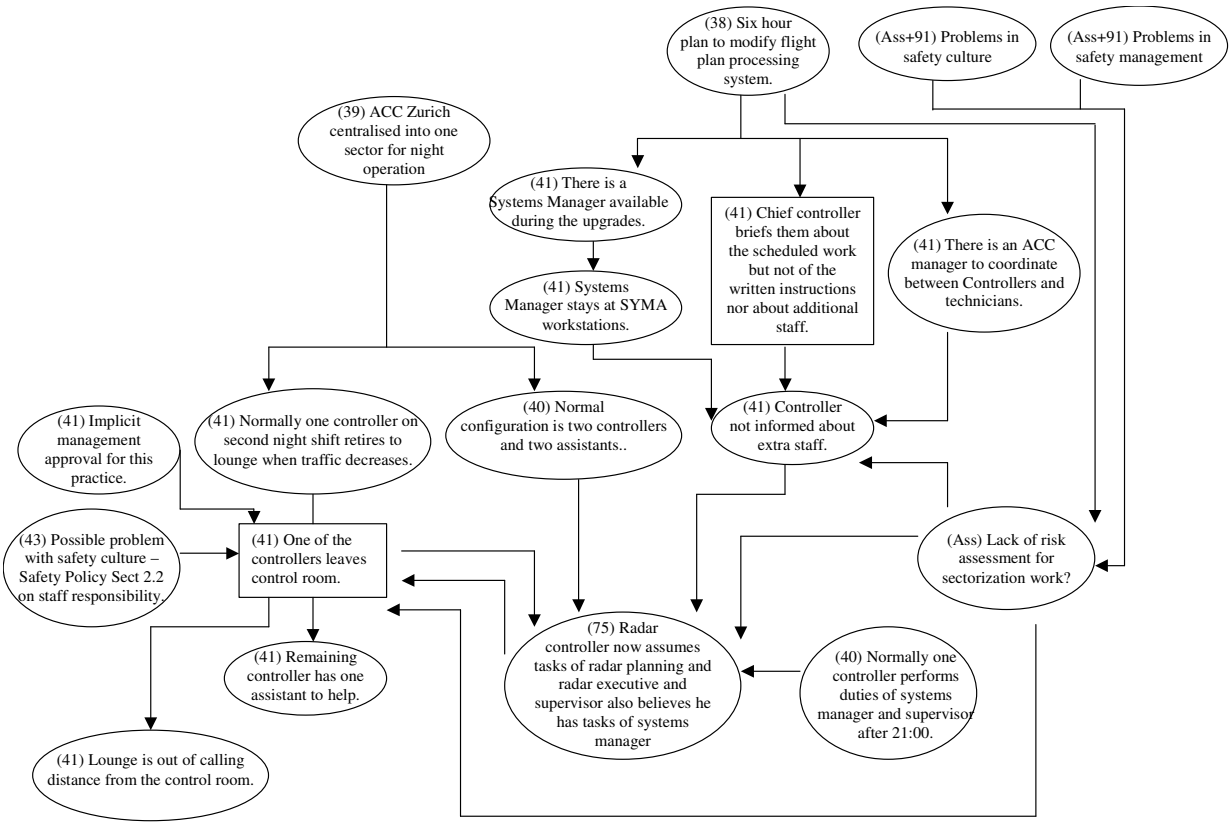

Figure 3: Contextual Factors Influencing the Human Systems Environment in the Zurich ACC

Figure 2 used a simplified ECF diagram to analyse the technical background to the Überlingen accident. In contrast, Figure 3 focuses more on personnel and staffing issues. As can be seen, ACC Zurich used a form of centralised operation during night operations. 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 the traffic died down so that he or she could rest in the lounge. During the accident, one of the controllers left the control room. This practice was known to management and there was no apparent

pressure to stop it hence there was an assumption of 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. The consequences of this practice were that the additional controller was now out of earshot from their remaining colleague and the remaining controller believed they only had one assistant to call on for help. It is difficult to determine what the other assistant was doing, as mentioned, two assistants should normally have supported the controllers. 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 SYMA workstation and 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 of the written instructions, mentioned above, nor about the additional staff. In consequence, a single controller was placed in a situation where they believed 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 recognise 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.

Recommendation 3:

Additional emphasis should be paid not simply to minimum staffing levels as recommended in the BFU report but also to a risk-based approach to the identification of situations that require additional staffing and to the need to inform staff when those additional resources are available.

Recommendation 4:

Additional emphasis should be placed not simply on minimum staffing levels (Recommendation 18/2004) but to *appropriate* staffing levels that match the maximum plausible task loading on controllers that might be anticipated from their operational and technical environment, considering the dangers of complacency and fatigue from idle operators during quiescence.

The Radar Controller's Role in the Accident

Figures 2 and 3 presented an overview of the technical and human resources that were available on the night of the accident and that were documented in the BFU report. In contrast, Figure 4 does on to look in more detail at the more immediate conditions and events that led to the accident.

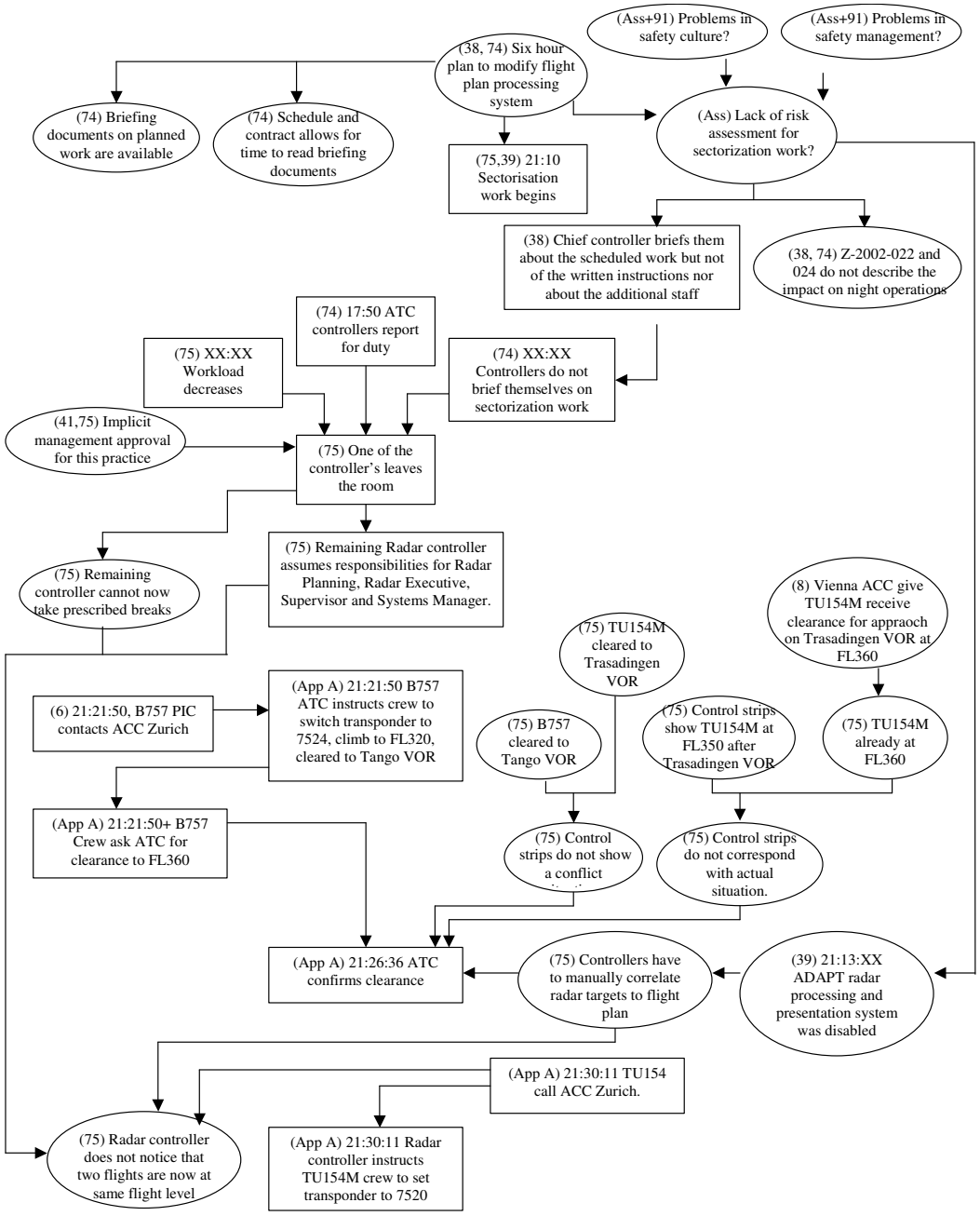

Figure 4: ECF Analysis of the Überlingen Accident - Clearance for B757 to Join TU154M at FL360

As can be seen, Figure 4 takes the analysis from the time at which the controllers report 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 are 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 lead 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 neighbouring centres 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.

It is important to emphasise 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.

Recommendation 5:

Additional emphasis should be placed on the concrete safety management techniques that might have identified the specific hazards in this accident well before the incident took place. These techniques include maintenance risk assessment according to the principles laid down in the ESSAR publications.

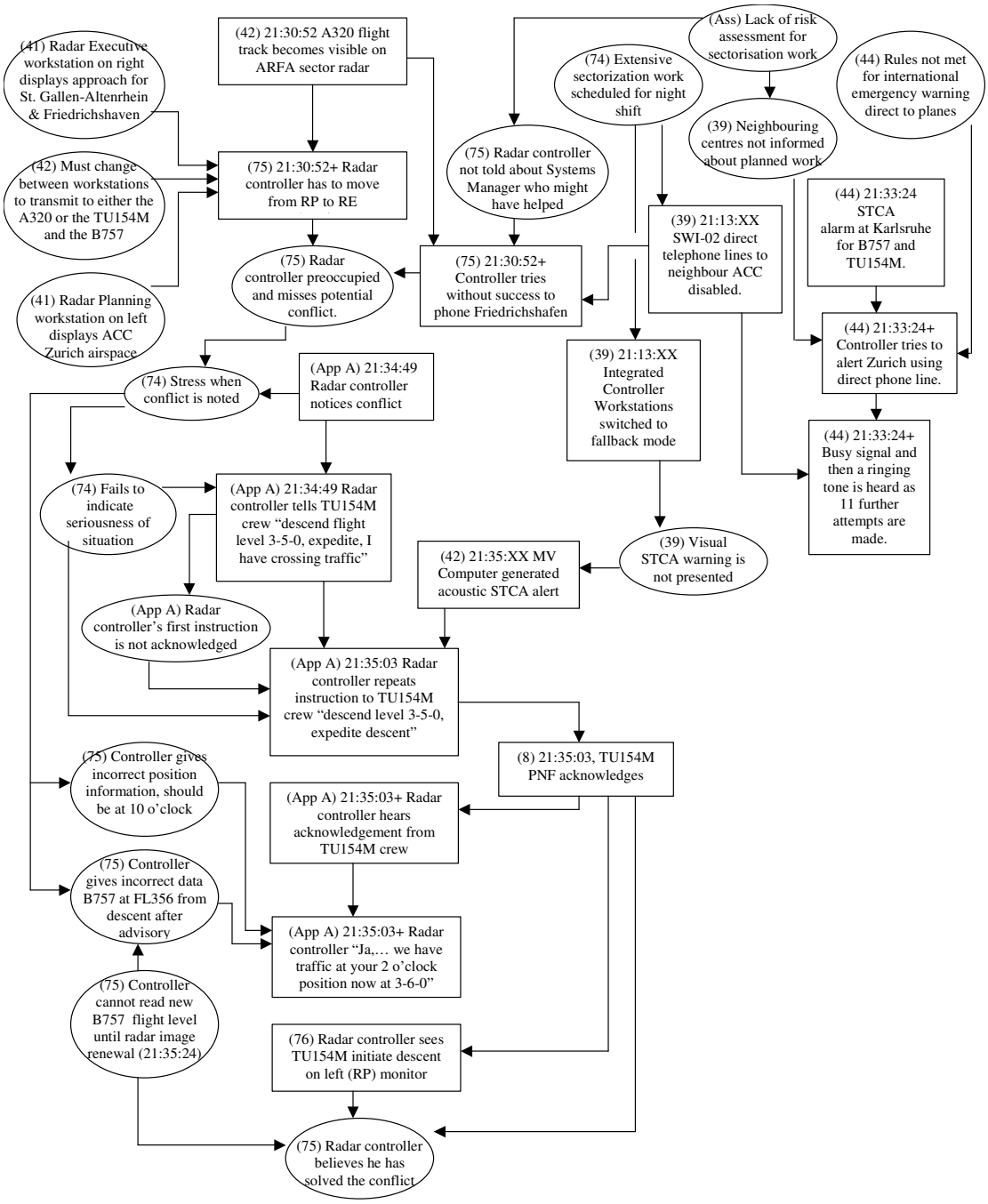

Figure 5: ECF Analysis of the Überlingen Accident – Radar Controller Notices and Attempts to Resolve Conflict

Figure 5 continues the ECF analysis of the BFU report 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 STCA alarm 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 warning at ACC Zurich. During these intervals 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 and this might have bought an additional two minutes warning compared to the time at which the controller began responding to the conflict. Figure 5 also illustrates another possible reason for the controller's failure to detect the potential conflict. An A320 flight enters the controllers area and he attempts to coordinate with Friedrichshaven. As we have seen, however, neither the controller nor the neighbouring areas were informed of the potential interruption to

the SWI-02 communications system and so valuable time was lost as the controller distributed his finite attention between the three aircraft and the associated tasks, including attempting to communicate with the neighbouring centres. The demands associated with these tasks were exacerbate by the layout of the controllers working positions as 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 recognising the conflict. This diagram 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.

Recommendation 6:
Any risk based assessment of the impact of large scale maintenance and upgrade activities should consider a range of plausible worst case scenarios especially where there may be common causes of 'failure'. In this case it was important to consider the combined effects of the loss of telecommunications as well as radar and flight plan correlation facilities rather than considering the consequences of each system loss in isolation.

Figure 5 also shows that the controller notices the conflict between the B757 and TU154M at 21:34:49. As mentioned previously, 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.

Recommendation 7:
A subsequent analysis of the accident should be conducted to identify the cognitive and perceptual cues that helped the controller to identify the potential conflict. It may have been through the Controller's direct observations of their radar displays, alternatively they may have been alerted to the conflict by indirect observations of the TCAS advisories that were issued in both cockpits at almost the same time the controller began to issue the initial descent instructions to the TU154M. Similarly, further attention to be paid to the protocols and procedures governing the transmission of location information such as the '2 o'clock' warning at 21:35:03. The BFU claim that this may have seriously disoriented the crew of the TU154M as they sought to resolve the TCAS alarm and yet nothing is stated about this in the existing recommendations.

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 further 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.

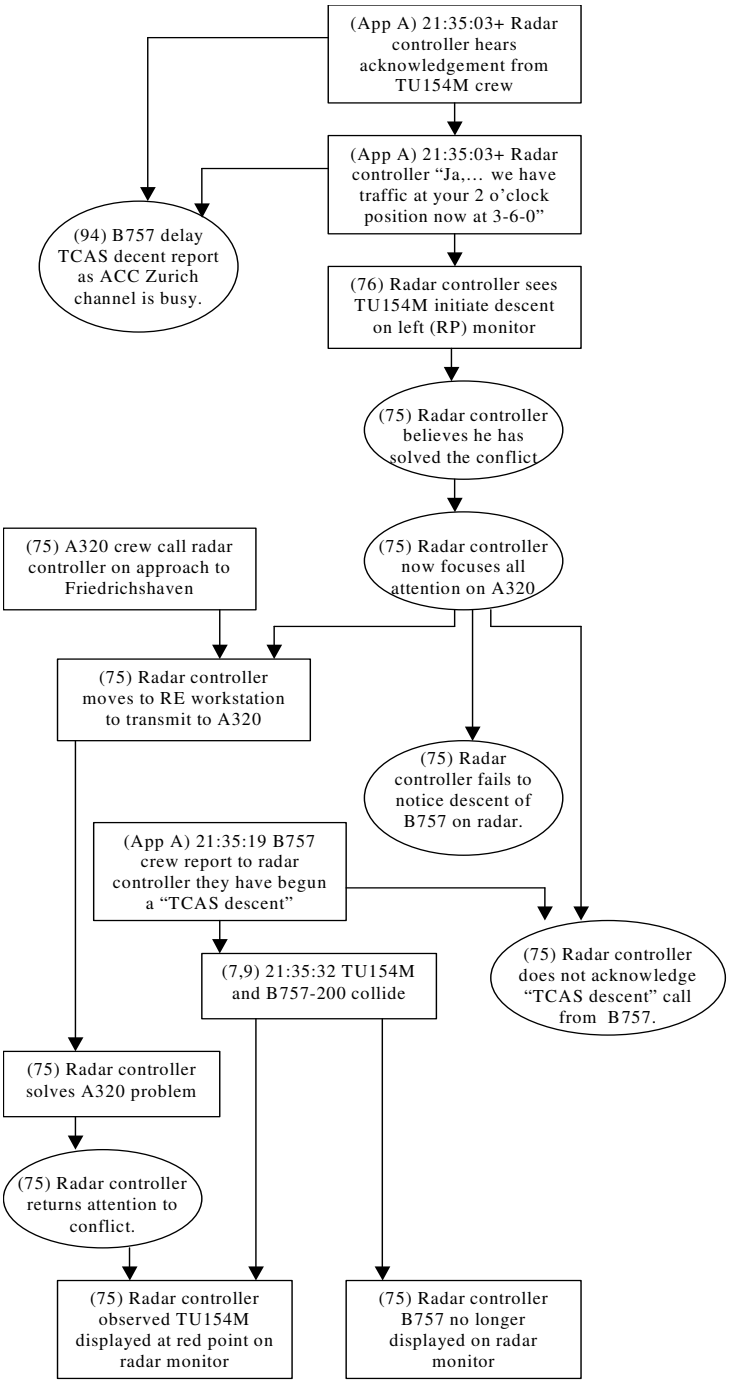

Figure 6: ECF Analysis of the Überlingen Accident – B757 Report TCAS Descent

The controller's preoccupation with the A320 and the split working positions can also be argued to explain his failure to notice the B757 crews' radio signal that they had begun 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:

> "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)

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. 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.

Recommendation 8:
Further thought should be given to the verbal protocols governing the exchange of information between controllers and the crews of all aircraft involved in a TCAS incident. Whenever possible channels of communication should be kept clear until all the parties involved have confirmed their immediate response to the warnings. The BFU recommendation 08/2004 that RA's be downlinked to ATC does not remove the need for such a verbal protocol given that even the revised ICAO guidelines offer crews discretion in the response to an advisory if they feel that to follow the TCAS alert would endanger safety.

Conclusions

This report documents the output from an initial analysis of the BFU report into the Überlingen mid-air collision. The investigation constructed a more detailed timeline of the events leading to the collision, from the perspective of both crews and the Radar Controller who was operating the position in Zurich ACC. This involved the compilation of additional details beyond the high-level summary that is provided in Appendix 2 of the BFU report. Once this timeline had been compiled, it was used to generate more complex Events and Causal Factors charts. These focussed on the influences that helped to shape the controllers interaction with the aircrews and with neighbouring centres during the crucial minutes before the collision. Our analysis identified a number of minor ambiguities and inconsistencies in the English language version of the report. It also extended the scope of the BFU investigation. The existing report focuses on issues surrounding the coordination of aircrew responses to TCAS advisories in the face of possibly conflicting instructions from Air Traffic Service personnel. It also provides a thorough account of safety management issues surrounding the staffing and operation of the Zurich center during major maintenance and upgrade operations. In contrast, the analysis in this report looks beyond the operating environment in the Zurich control room on the night of the accident. Greater emphasis is placed on adequate preparation for what was extensive technical procedures that deprived the controllers of necessary support and created an 'error inducing' environment. In particular, the BFU report provides few insights into the risk assessment procedures that should be used before any similar upgrades should be attempted in the future. The final stages of this project will look at the specific safety management and risk assessment techniques that might have been used to alert senior management to the dangers that were created by the planned upgrades at ACC Zurich.

It is important to stress that we have focussed on the controllers' perspective in this report. The role of both crews and the impact of ACAS/TCAS have already been well covered by the BFU. It is also important to stress that this report is not intended to be a criticism of the BFU report. They conducted a thorough and detailed investigation under difficult circumstances and their recommendations have clearly made a significant contribution to aviation safety. However, our aim has been to go beyond the existing recommendations and extract any additional lessons that might be learned from this very unfortunate incident. Our secondary aim has also been to ensure that the recommendations made by the BFU were supported by either systemic or immediate causes.

Summary of Findings:
The BFU report contains two recommendations that are not supported by their causal analysis, although the evidence provided in the report supports them. There recommendations are as follows:

Safety Recommendation No. 01/2003
The Federal Office for Civil Aviation (FOCA) should ensure that the air traffic control service provider issues and implements procedure to undertake maintenance work on the ATC Systems stipulating operational effects and available redundancies. The procedure shall include the following aspects:

- Stipulating the detailed responsibilities of the Operational Division and the Technical Division.
- Personnel reserve planning of the operational staff for maintenance work on the ATC Systems.
- Timely dissemination of procedure to the controllers, in order to prepare them to deal with the situations.
- Establish and implement the checklists for the maintenance as well operational staff, when maintenance work on the ATC Systems is undertaken, to enhance the safety net.
- Selection of best possible time from operational aspects for the maintenance work on the ATC Systems.

Safety Recommendation No. 11/2004
The FOCA should ensure that the air traffic control service provider equips air traffic control units with telephone systems which in case of a failure or shutdown of the main telephone system reroutes incoming telephone calls automatically to the bypass telephone system.

It is difficult to be sure why these recommendations are not supported by the immediate and systemic causes mentioned in the BFU report. However, our analysis suggests that greater attention ought to have been paid to the planning and management of the SYCO upgrades. In particular we could argue that a more sustained form of risk assessment might should have been used before the work was undertaken.

In addition, our analysis has identified the following additional recommendations:

Additional Recommendation 1: Controllers should be made more aware of the role of STCA in the Überlingen accident as a reminder of the strengths and weaknesses of this tool. Our analysis and that of the BFU reinforces the role of STCA as a 'safety net' and not as an absolute defense against adverse events.

Additional Recommendation 2: Additional emphasis should be paid to a risk-based approach to the identification and dissemination of information about the impact of necessary upgrades on the ATM infrastructure.

Additional Recommendation 3: Additional emphasis should be paid not simply to minimum staffing levels as recommended in the BFU report but also to a risk-based approach to the identification of situations that require additional staffing and to the need to inform staff when those additional resources are available.

Additional Recommendation 4: Additional emphasis should be placed not simply on minimum staffing levels (Recommendation 18/2004) but to *appropriate* staffing levels that match the maximum plausible task loading on controllers that might be anticipated from their operational and technical environment, considering the dangers of complacency and fatigue from idle operators during quiescence.

Additional Recommendation 5: Additional emphasis should be placed on the concrete safety management techniques that might have identified the specific hazards in this accident well before the incident took place. These techniques include maintenance risk assessment according to the principles laid down in the ESSAR publications.

Additional Recommendation 6: Any risk based assessment of the impact of large scale maintenance and upgrade activities should consider a range of plausible worst case scenarios especially where there may be common causes of 'failure'. In this case it was important to consider the combined effects of the loss of telecommunications as well as radar and flight plan correlation facilities rather than considering the consequences of each system loss in isolation.

Additional Recommendation 7: A subsequent analysis of the accident should be conducted to identify the cognitive and perceptual cues that helped the controller to identify the potential conflict. It may have been through the Controller's direct observations of their radar displays, alternatively they may have been alerted to the conflict by indirect observations of the TCAS advisories that were issued in both cockpits at almost the same time the controller began to issue the initial descent instructions to the TU154M. Similarly, further attention to be paid to the protocols and procedures governing the transmission of location information such as the '2 o'clock' warning at 21:35:03. The BFU claim that this may have seriously disoriented the crew of the TU154M as they sought to resolve the TCAS alarm and yet nothing is stated about this in the existing recommendations.

Additional Recommendation 8: Further thought should be given to the verbal protocols governing the exchange of information between controllers and the crews of all aircraft involved in a TCAS incident. Whenever possible channels of communication should be kept clear until all the parties involved have confirmed their immediate response to the warnings. The BFU recommendation 08/2004 that RA's be downlinked to ATC does not remove the need for such a verbal protocol given that even the revised

ICAO guidelines offer crews discretion in the response to an advisory if they feel that to follow the TCAS alert would endanger safety.

Appendix A: Detailed Timeline of the Überlingen Accident

As mentioned, the Überlingen report contains a high level timeline of the events that led to the collision. This is presented in Appendix 2 of the official report and runs from 21:21:50 until 21:35:32. The timeline provides a good general overview of the events leading to the accident. However, it does not cover many of the events that created the context for the collision and which occurred before the B757 and TU154M entered Zurich ACC airspace. Similarly, it focuses on the events that occurred in both cockpits and arguably neglects the controller's perspective. The following pages present an extended timeline that was then used as input for the subsequent Event and Causal Factors analysis of the BFU report.

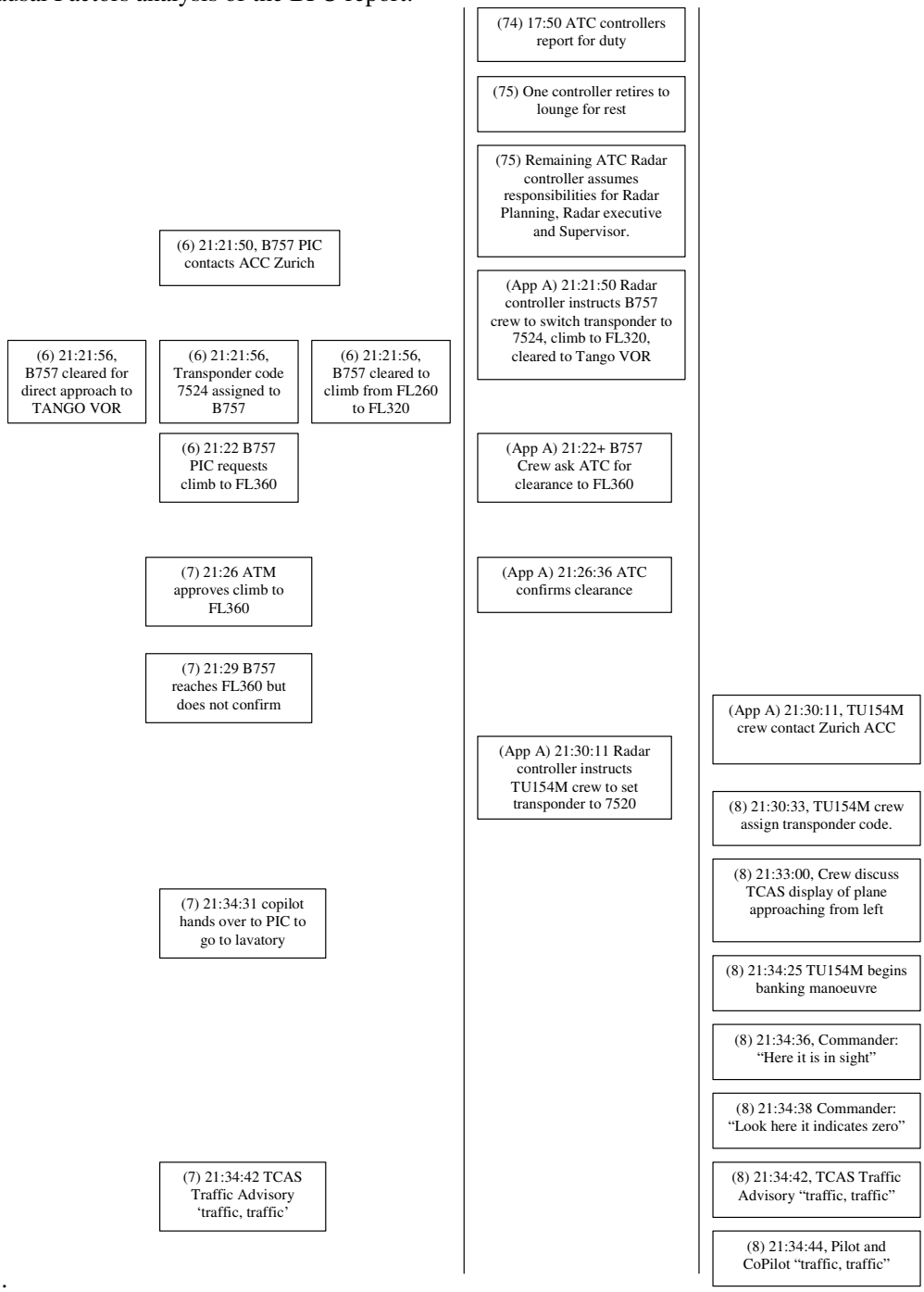

Figure A1: Extended Timeline from Start of Controllers' Shift (17:50)

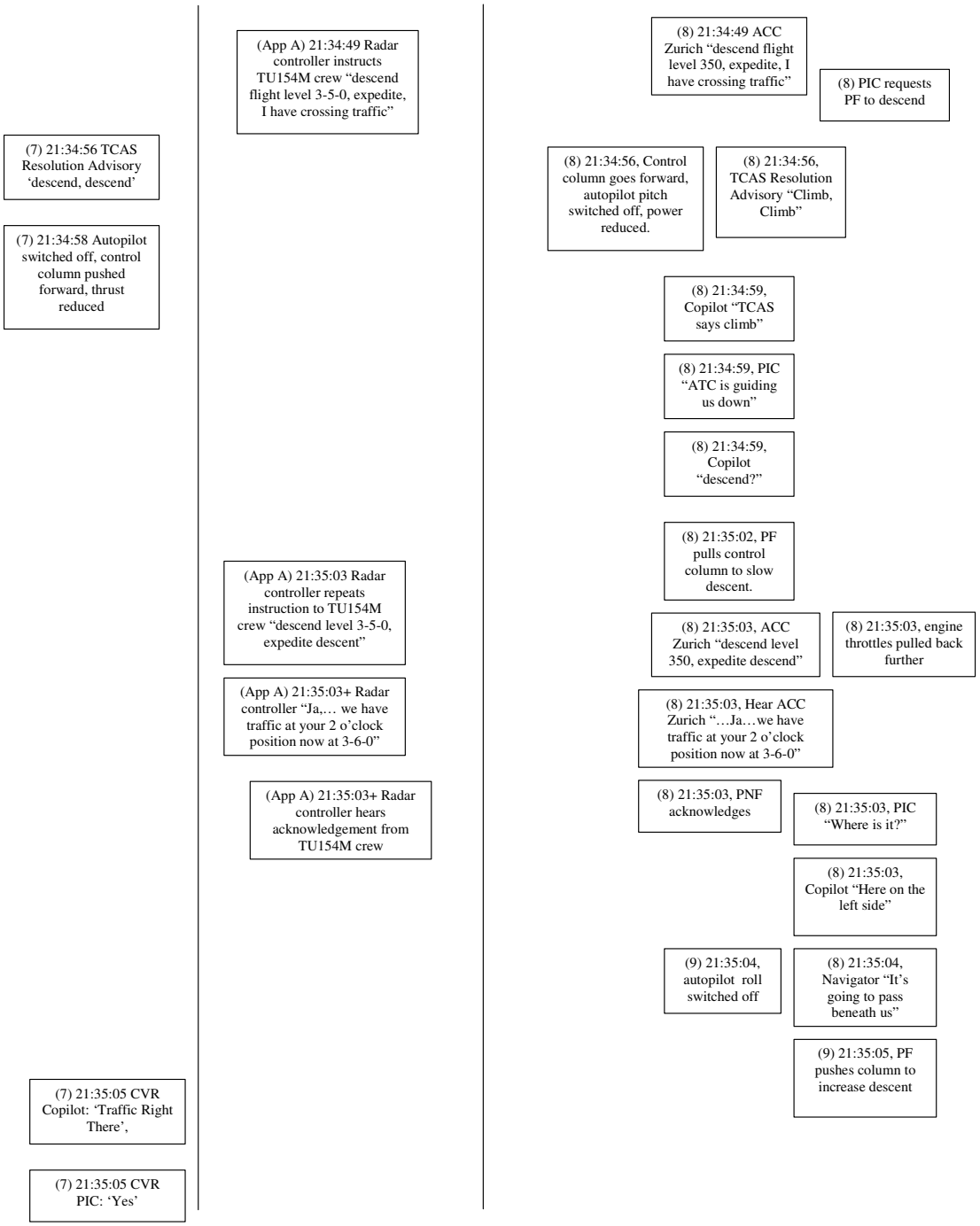

Figure A2: Extended Timeline from the Controller's Initial Descent Instruction (21:34:49)

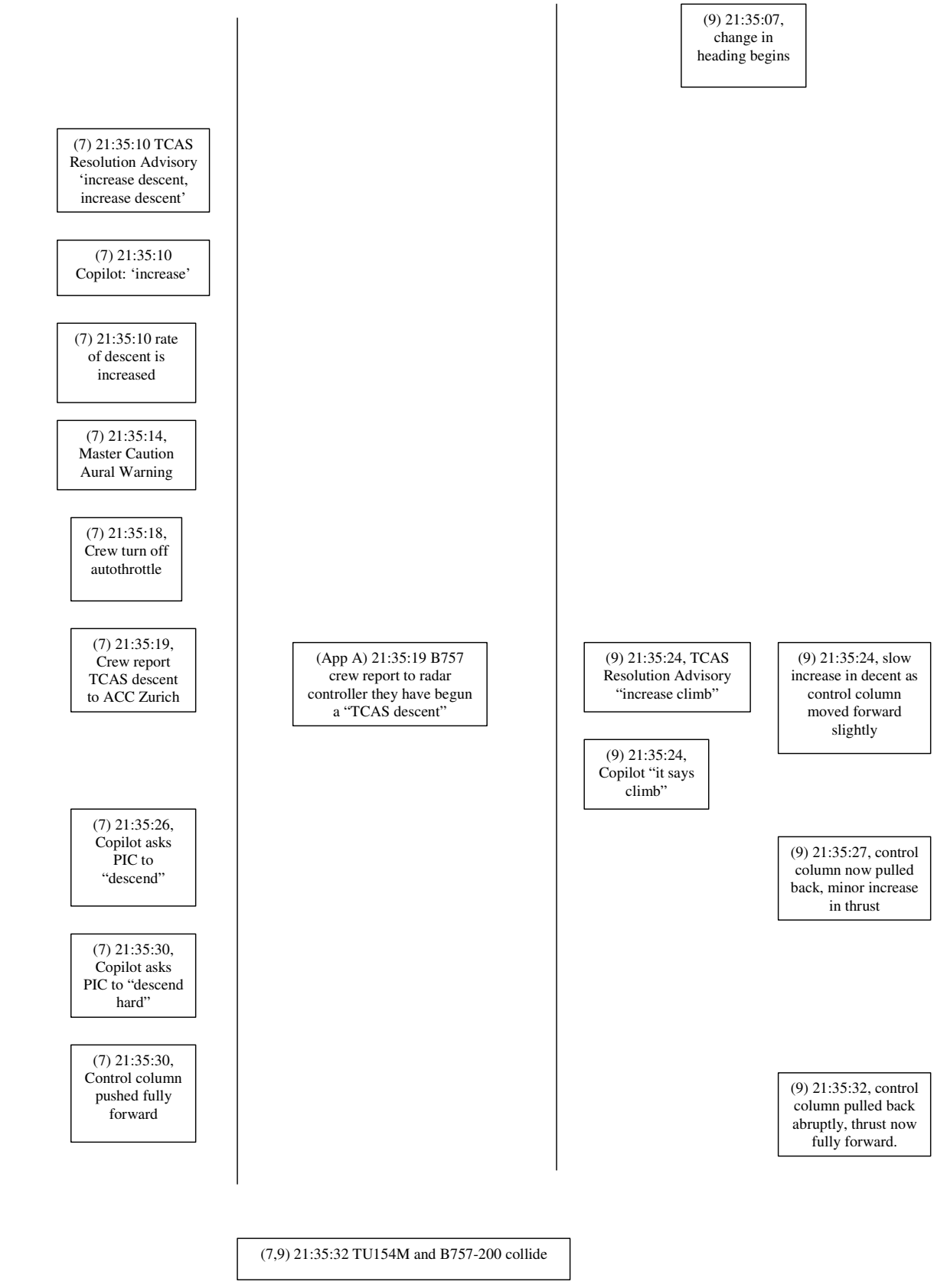

Figure A3: Extended Timeline from the TU154M's Change in Heading (21:35:07)

Technical Report B:

Incorporating Deliverable 3

(Version 1: 17/12/2004)

Contract C/1.369/HQ/SS/04

Executive Summary of Technical Report B

This is the second report of two issued under this contract. The first report identified recommendations in the BFU report that were not fully supported by their causal analysis. The first report also used an Events and Causal Factors analysis to identify eight additional recommendations from the BFU report. The principle insight from all of this work was that the BFU did good work in analysing the role of ACAS/TCAS in the two planes. However, less attention was paid to the inadequate risk assessments that exposed the controllers to extreme operational demands during the SYCO systems upgrade. This report builds on the findings of the initial document. In particular, it goes on to look at the role that Safety Management Systems played in the accident. We concur with the BFU that the Swiss authorities had well-documented procedures and principles that would encourage the development of a sound Safety Management System. These principles were in accordance with ICAO and EUROCONTROL guidelines. However, the Swiss ATM organisations lacked the experience and the personnel to implement those procedures. Partly as a result of this opportunities were missed to learn from two AIRPROX incidents that had similarities to the events before the Überlingen accident. A number of additional recommendations are presented in this report that build on those recommendations already provided in Technical Report A.

Prepared by:

Prof. Chris Johnson
217, Wilton Street, North Kelvinside, Glasgow, G20 6DE, Scotland, UK.
Johnson@dcs.gla.ac.uk (Email), +44 141 330 6053 (Tel.), +44 141 330 4913 (Fax)

Introduction

The EUROCONTROL Strategic Safety Action Plan (SSAP) has initiated a number of reviews into the BFU Überlingen Accident Report. The intention behind this study is to determine whether employing a team of accident investigators to study the existing report can derive any additional findings. The key objectives for this study are:

1. to show how existing recommendations relate to root causes identified in the existing report. The main focus will be to use Events and Causal Factors diagrams to draw out the root causes from the report and then to relate them to the recommendations. This choice of this method is justified because it provides relatively accessible diagrams that can readily be inspected to trace the information in the report back to particular recommendations. EUROCONTROL has used similar diagrams to model human error and systems failure in ATM incidents, for example in HUM.ET1.ST13.3000-REP-02 Human Factors in the Investigation of Accidents and Incidents.

2. *to use recognised accident analysis techniques to identify further recommendations from this accident.* The ECF model developed in the previous stage of analysis can also be used to help identify additional recommendations. This will be done using the associated reasoning techniques that are part of this method. Additional root causes can be identified by examining each element of the diagram and asking whether or not the accident could have been avoided if that event had not occurred. If the answer is yes then the event or condition becomes a candidate for further inspection.

3. *to review the existing BFU report and other reports into this accident dealing with the associated safety management systems to extend the scope of objective (2).* This final stage of the project will look more closely at the findings from the second stage of analysis. Rather than focussing on the BFU report alone, this stage will look at the wider investigatory process in the context of SMS development and will refer to investigatory practices in other countries. In particular, comparisons will be drawn with the FAA and Canadian TSB's guidelines on SMS development.

There are three deliverables associated with this project. Each represents the output of one of the stages identified in the previous section. The first is to deliver an analysis of the mapping from recommendations to root causes in the BFU report. The second is to identify appropriate additional recommendations. Both of these deliverables were documented in Technical Report A. For convenience, the following section provides an executive summary of the output from this work. This report represents the final deliverable associated with this contact. It links the information derived from objectives 1 and 2 to associated work on safety management system guidance within ATM.

Summary from Technical Report A

Technical Report A first determined whether any of the recommendations from the BFU were not adequately supported by the associated causal analysis. The BFU report into the Überlingen collision identified a number of immediate causes for the accident. These can be summarised as follows, all page numbers in the remainder of this report refer to the official BFU English language translation of the original German report:

• (Immediate Cause 1) "The imminent separation infringement was not noticed by ATC in time. The instruction for the TU154M to descend was given at a time when the prescribed separation to the B757-200 could not be ensured anymore". (BFU page 112)

• (Immediate Cause 2) "The TU154M crew followed the ATC instruction to descend and continued to do so even after TCAS advised them to climb. This manoeuvre was performed contrary to the generated TCAS RA". (BFU page 112)

In addition, the BFU also identified a number of less immediate systemic causes:

• (Systemic Cause 1) "The integration of ACAS/TCAS II into the system aviation was insufficient and did not correspond in all points with the system philosophy. The regulations concerning ACAS/TCAS published by ICAO and as a result the regulations of national aviation authorities, operational and procedural instructions of the TCAS manufacturer and the operators were not standardised, incomplete and partially contradictory". (BFU, page 112)

• (Systemic Cause 2) "Management and quality assurance of the air navigation service company did not ensure that during the night all open workstations were continuously staffed by controllers". (BFU, page 112)

• (Systemic Cause 3) "Management and quality assurance of the air navigation service company tolerated for years that during times of low traffic flow at night only one controller worked and the other one retired to rest." (BFU, page 112)

The BFU report contains two recommendations that are not supported by their causal analysis, although the evidence provided in the report supports them. There recommendations are as follows:

Safety Recommendation No. 01/2003
The Federal Office for Civil Aviation (FOCA) should ensure that the air traffic control service provider issues and implements procedure to undertake maintenance work on the ATC Systems stipulating operational effects and available redundancies. The procedure shall include the following aspects:

- Stipulating the detailed responsibilities of the Operational Division and the Technical Division.
- Personnel reserve planning of the operational staff for maintenance work on the ATC Systems.
- Timely dissemination of procedure to the controllers, in order to prepare them to deal with the situations.
- Establish and implement the checklists for the maintenance as well operational staff, when maintenance work on the ATC Systems is undertaken, to enhance the safety net.
- Selection of best possible time from operational aspects for the maintenance work on the ATC Systems.

Safety Recommendation No. 11/2004
The FOCA should ensure that the air traffic control service provider equips air traffic control units with telephone systems which in case of a failure or shutdown of the main telephone system reroutes incoming telephone calls automatically to the bypass telephone system.

It is difficult to be sure why these recommendations are not supported by the immediate and systemic causes mentioned in the BFU report. However, our analysis suggests that greater attention ought to have

been paid to the planning and management of the SYCO upgrades. In particular we could argue that a more sustained form of risk assessment should have been used before the work was undertaken. In addition, our analysis identified the following recommendations:

Additional Recommendation 1: Controllers should be made more aware of the role of STCA in the Überlingen accident as a reminder of the strengths and weaknesses of this tool. Our analysis and that of the BFU reinforces the role of STCA as a 'safety net' and not as an absolute defense against adverse events.

Additional Recommendation 2: Additional emphasis should be paid to a risk-based approach to the identification and dissemination of information about the impact of necessary upgrades on the ATM infrastructure.

Additional Recommendation 3: Additional emphasis should be paid not simply to minimum staffing levels as recommended in the BFU report but also to a risk-based approach to the identification of situations that require additional staffing and to the need to inform staff when those additional resources are available.

Additional Recommendation 4: Additional emphasis should be placed not simply on minimum staffing levels (Recommendation 18/2004) but to *appropriate* staffing levels that match the maximum plausible task loading on controllers that might be anticipated from their operational and technical environment, considering the dangers of complacency and fatigue from idle operators during quiescence.

Additional Recommendation 5: Additional emphasis should be placed on the concrete safety management techniques that might have identified the specific hazards in this accident well before the incident took place. These techniques include maintenance risk assessment according to the principles laid down in the ESSAR publications.

Additional Recommendation 6: Any risk based assessment of the impact of large scale maintenance and upgrade activities should consider a range of plausible worst case scenarios especially where there may be common causes of 'failure'. In this case it was important to consider the combined effects of the loss of telecommunications as well as radar and flight plan correlation facilities rather than considering the consequences of each system loss in isolation.

Additional Recommendation 7: A subsequent analysis of the accident should be conducted to identify the cognitive and perceptual cues that helped the controller to identify the potential conflict. It may have been through the Controller's direct observations of their radar displays, alternatively they may have been alerted to the conflict by indirect observations of the TCAS advisories that were issued in both cockpits at almost the same time the controller began to issue the initial descent instructions to the TU154M. Similarly, further attention to be paid to the protocols and procedures governing the transmission of location information such as the '2 o'clock' warning at 21:35:03. The BFU claim that this may have seriously disoriented the crew of the TU154M as they sought to resolve the TCAS alarm and yet nothing is stated about this in the existing recommendations.

Additional Recommendation 8: Further thought should be given to the verbal protocols governing the exchange of information between controllers and the crews of all aircraft involved in a TCAS incident. Whenever possible channels of communication should be kept clear until all the parties involved have confirmed their immediate response to the warnings. The BFU recommendation 08/2004 that RA's be downlinked to ATC does not remove the need for such a verbal protocol given that even the revised ICAO guidelines offer crews discretion in the response to an advisory if they feel that to follow the TCAS alert would endanger safety.

The remaining sections of this report go on to review the role that Safety Management Systems played in the Überlingen accident. The results of this analysis are then placed in the context of existing guidance and recommendations both within Europe and the United States.

The BFU's Analysis of Safety Management Systems in the Überlingen Accident

The BFU report identifies the safety management systems and safety culture as key issues in their analysis of the Überlingen accident. In particular, they refer to the ICAO Human Factors Guidelines for Safety Audits Manual (Doc 9806 AN/763, 2002)which states that "Safety culture in aviation refers to the personal dedication and accountability of individuals engaged in any activity that has a bearing on the safety of flight operations. It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters". They go on to argue that safety culture related to attitudes and behaviors as well as organizational techniques, such as Safety Management Systems. A strong safety culture will, therefore, result in both individuals and organizations associating a high priority with safety and that they will then act on that basis. Managers play a key role in all of this because they create the environment in which it is possible to identify those systems and working practices that must be monitored and improved if safety is to be ensured. The BFU report contains several sections that describe the safety culture and the associated Safety Management Systems that were in place within the Air Navigation Service of Switzerland at the time of the accident. For example, on page 43 of the report they cite sections from the company's 'Safety Policy' published in October 2001. The BFU found that the following principles complied with the different requirements published by ICAO, Eurocontrol and the Bundesamt für Zivilluftfahrt (BAZL). They were also argued to go beyond those existing requirements at the time of the accident:

2. Principles:

2.1 The safety of Air Navigation will be given the highest priority. An explicit, pro-active approach to Safety Management will ensure reasonable assurance of maintaining optimum levels of safety in the development, implementation and continued function of the […] operation.

2.2 All staff have an individual responsibility for their own actions whilst Managers are responsible for the Safety Performance of their own divisions.

2.3 All staff members performing activities with safety related implications will be adequately trained, motivated and competent to undertake the tasks required of them, and properly licensed where appropriate.

3. Description:

3.1 Quantitative Safety Levels – meeting appropriate and agreed target levels of safety – will be derived for all systems.

3.2 New systems and changes to existing systems, operations and procedures (including Engineering systems) will be regularly assessed for their safety significance and safety criticality. The results of these safety assessments will be documented in an appropriate manner allied to the requirements of the established quality environment.

3.3 To provide Safety Assurance, Safety Audits will be performed routinely in order to confirm conformance with applicable parts of the Safety Management System and to provide assurance to Managers that the continued operations and risks are identified, conform to appropriate safety levels and are being adequately managed.

3.4 Reflecting best Safety Practice – these Safety Audits will enable appropriate measures to be taken for the attainment and maintenance of the agreed Target Safety Levels.

3.5 […]

3.6. A Safety Culture will be promoted which will aim, amongst other objectives, at disclosing mistakes and motivating all staff members to endeavour to constantly improve safety through their own individual contributions. An integral part of this enhancement may be the adoption of a unique and non punitive company confidential reporting scheme.

> 3.7 An enhanced Safety Culture will ensure that the lessons and experience gained from safety related investigative processes will be widely distributed and actioned to minimize the residual risk of reoccurrence.

The BFU argued that the Air Traffic Service provider used Safety Audits as the main mechanism for managing safety within their organisation. These are mentioned in the 'Safety Policy' under item 3.3 in the previous quotation. However, the BFU argued that staff shortages within the ATM service provider had placed undue strain on the organisation 'it influenced maintenance and desired improvements of systems and the required staffing levels and training' (p. 90). This BFU analysis is extremely important given the findings of the earlier stages of this contract. We have argued that there was inadequate risk assessment prior to the SYCO system upgrade. The BFU do not form this connection, however, their analysis of the safety management structure within the Air Traffic Service provider would indicate that staff shortages were an important factor in this potential vulnerability. The BFU five 'problem areas' in the Safety Management Systems that were being operated at the time of the accident.

Problem area 1: Delays in Establish a Centre of Competence
After leaving state control, the service provide became an independent company. It realised the need to revise its safety management structure and, therefore, created a Centre of Competence to fill any existing omissions. The main responsibilities for this organisation were safety, quality, audit and risk management. The BFU argued that audit and quality assurance were already well understood by the service provider when the accident occurred. However, they lacked specialist risk assessment and safety expertise. Rather than call on external help they elected to develop appropriate systems themselves. The BFU report contains two critical sentences which are essential to understanding the Air Traffic Management involvement in this accident and which arguably do not have enough prominence in the existing document and its associated recommendations; "The Safety Policy (please refer to 1.18.1) clearly suggests the CoC should have been formally involved in the planned structure change of the upper airspace which did not happen. Without knowledge of the planned sectorisation work the Risk Manager could not conduct a quantitative risk assessment and mitigation process" (BFU page 91).

Problem area 2: Staffing Shortages
Staffing problems created pressures on staff and management either to increase their workload or to reduce the quality of service that had traditionally been provided. This had profound effects on staff morale. Training suffered and long-term rostering was difficult as recruitment failed to keep pace with the demands for new staff.

Problem area 3: Inadequate ATCO Training and Advanced Training in 'Emergency' Situations
There is a paradox in the BFU report. Not only does it criticise the risk assessment practices of the Air Traffic Service provider. It also uses a form of "20-20" hindsight to criticise the training of Air Traffic Control Officers on the basis of the problems that emerged during the Überlingen accident. There seems to be an assumption that because errors were made then training must have been to blame. The focus of the first report in this contract has, however, been to focus more on the problems of risk assessment. Even if the relevant personnel had been better trained there is little evidence and few guarantees that they would have been able to cope with the demands that their operating environment placed on them during this accident. For completeness sake, it is important to mention that the BFU criticise the training of ATC personnel in the operation of fallback mode. There was insufficient practical exposure to this mode of operation. The documentation was also inadequate. The BFU argued that "although operating in fallback mode is not overly problematic or inherently unsafe it must be understood how the system's defences are understood" (BFU page 91). This statement is contentious. Certainly by the standards in other industries, such as nuclear power or military operations, it would be difficult to argue that the fallback mode is inherently 'safe' even if controllers have a complete understanding of the available defences. Recall also that these defences changed over time as the SWI-02 communications system was gradually brought back into service without the controller being informed. The BFU report goes on to argue that the night controllers were expected to perform the functions of the supervisor ("DL") but had not been trained for this role. The twice-yearly refresher courses could only be held once a year because

of staffing shortages. Similarly, it was recognised that there was no comprehensive training in emergency procedures nor was there an adequate simulation facility. The company also failed to provide adequate documentation for these emergency procedures.

Problem area 4: Inadequate Night Staffing Levels and Single Man Operating Procedures
Again, the BFU report identifies particular contextual issues that may have contributed to the Überlingen accident. It is then argued that these are symptomatic of problems in the underlying safety culture. For example, there were no written regulations about the night shift. The practice of only rostering two controllers was an outcome of the staffing problems during the nightshift. The previous practice had been to use three controllers with one taking a break. This break schedule continued even when the rostering only allocated two controllers to the shift. Technical report A in this contract discusses the consequences of this practice. The BFU also identified regulations for Single Manned Operation that should only have been applied during the day and not at night. The situation facing the controller violated the day-time SMOP rules in several ways. For example, he did not have the support of a supervisor, which was a requirement for day-time single manned operation. Similarly, it was not possible for the controller to ask for help from a colleague as should have been the case because they were resting in a lounge that was too far away for their requests to be heard.

Problem area 5: Poor Internal Reporting of Safety Incidents
The BFU report argues that some controllers were reluctant to report safety concerns for a fear that they might suffer some form of punitive retribution. The BFU argued it was "inoperative as a confidential internal reporting system for identifying error sources". There is also evidence that lessons had not been learned effectively from more formalised reporting systems. For example, Zurich ACC had experienced two AIRPROX incidents during the Single Man Operating Procedures described in the previous paragraph. Concerns had been raises by the Swiss BFU and by the Swiss Federal Office of Civil Aviation. Zurich had, however, argued that these practices were common in other European states and internationally. The BFU argue that ACC Zurich failed to carry out a sustained risk assessment and, therefore, did not identify appropriate mitigation measures.

The BFU report closes by identifying poor Safety Management Systems as one of the systemic causes of the Überlingen accident. They then used this causal argument to justify one of the recommendations directed at the Swiss Federal Office for Civil Aviation:

> (Systemic Cause 2) "Management and quality assurance of the air navigation service company did not ensure that during the night all open workstations were continuously staffed by controllers". (BFU, page 112)
>
> **Safety Recommendation No. 17/2004**
> The Swiss Federal Office for Civil Aviation (FOCA) should ensure that the air traffic service provider takes appropriate action to assure an effective operation of their safety management system in as much as that international requirements (ICAO SARPs, Eurocontrol ESARRs) are assured, and appropriate safety strategies, management techniques and quality procedures are incorporated and evaluated. (BFU, page 113)

This recommendation illustrates the key point about Safety Management Systems in the BFU report. The Swiss agency's existing safety "policy and principles were in compliance with the requirements published by ICAO, Eurocontrol and the Bundesamt für Zivilluftfahrt (BAZL) and included already future requirements which were not mandatory at that time" (BFU, page 90). However, it was the implementation and monitoring of the safety policy that lay at the heart of this accident. The Swiss Federal Office for Civil Aviation must ensure the effective operation of those principles and procedures rather than force any revision to those requirements. In consequence, organisations such as EUROCONTROL and the ICAO might benefit greatly by supporting the monitoring of enforcement and operation rather than the development of new requirements for Safety Management Systems.

Additional Recommendation 9:
The Überlingen accident was caused by failures in the safety management systems that did not ensure the use of appropriate risk assessment techniques prior to the SYCO upgrade. Appropriate procedures and principles were in place within Swiss Air Traffic Management and it seems clear that had these been followed then the controllers might not have been exposed to such demanding operating conditions. It follows that EUROCONTROL and the ICAO might, therefore, usefully provide additional services in helping organisations implement these good practices and where appropriate might assist national regulators in monitoring their implementation.

Additional Recommendation 10:
The Überlingen accident was pre-dated by two AIRPROX incidents in Zurich ACC that eloquently illustrated the dangers of Single Man Operating Procedures even under more benign circumstances that existed on the night of the accident. EUROCONTOL ESSAR guidelines require that such incidents should normally trigger a formal risk assessment and yet this was not done in either of these cases. It is difficult to be certain about why the guidelines were not followed here. The BFU report does not contain enough detail and this issue certainly merits further investigation. These AIRPROX incidents represent valuable learning opportunities that were missed *before* the Überlingen accident.

Links Between the Safety Management Analysis and Accident Precursors

The previous pages have summarised the BFU's analysis of the role of Safety Management Systems and safety culture in the Überlingen accident. This analysis has helped to explain some of the reasons why an adequate risk assessment was not conducted prior to the upgrade work at ACC Zurich. The following pages extend this analysis in several ways. Firstly, Events and Causal Factors diagrams are again used to link the higher level and general observations in the BFU report to specific details in the lead up to the collision. This adds detail to the information contained in the BFU report by going down a level to look at the interaction between safety culture and specific events or causal factors that were identified in Technical Report A. Subsequent sections take the opposite approach. Rather than looking in more detail at this specific incident, the intention is to look more widely at the practices in Swiss Air Traffic Safety Management in relation to the guidelines and policies of other national and international organisations.

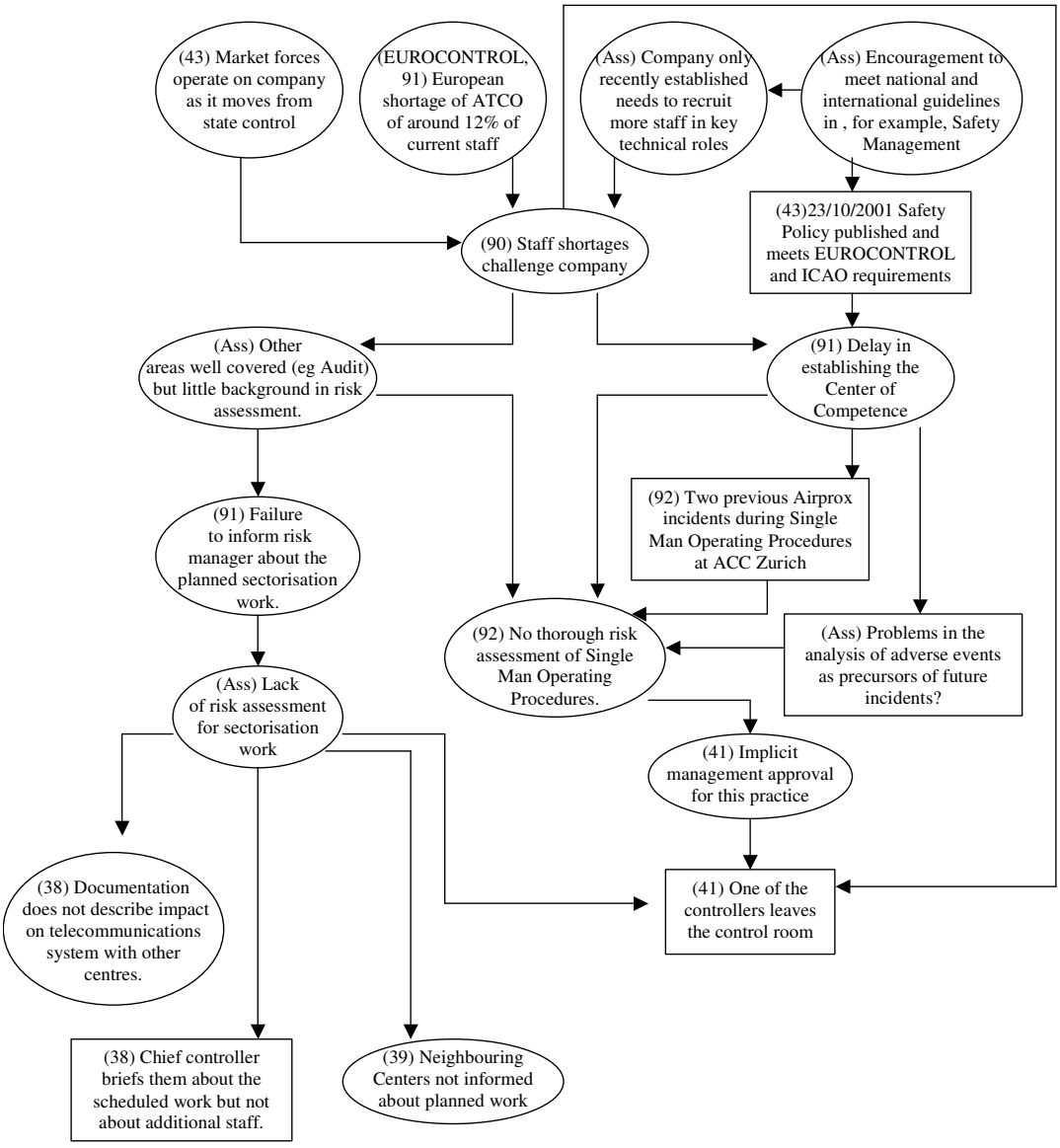

Figure B-1: Interaction Between Safety Management System and Lead-Up to the Accident

Figure B-1 presents a simplified form of Events and Causal Factors analysis, initially pioneered by the US Department of Energy. This is the notation that was used to sketch the events leading to the Überlingen accident in Tedchnical Report A. Previous EUROCONTROL projects have used similar diagrams to model human error and systems failure in ATM incidents, for example in HUM.ET1.ST13.3000-REP-02 Human Factors in the Investigation of Accidents and Incidents. Ellipses are used to denote contributory factors that combine to make events more likely. Events, as before, 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 Figure B-1, as in the previous report, some events are annotated with 'Ass' to explicitly represent any assumptions that were not explicitly referenced in the BFU report.

As can be seen, a number of contributory factors can be identified as potential causes of the staff shortage within the Air Traffic Service Provider. The company 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. It also had to respond to both 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 the Centre of Competence. However, as can be seen from Figure B-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 can be seen from Figure B-1 and from the previous ECF diagrams in 2 to 5 of Technical Report A this lack of risk assessment had profound consequences. Some of these are illustrated in B-1 to form a concrete link with the previous analysis. For instance, we have shown that the lack of risk assessment may have led to the publication of documentation such as Z-2002-022 and 024 that did not describe the impact of the upgrade on the SWI-02 communications system with other neighboring centers. Similarly, B-1 shows that the lack of any risk assessment may have contributed to the chief controllers' briefing, which did not mention the additional staff that were available during the maintenance work. We have not shown the impact that any risk assessment might have had on the choice of procedures used to perform the upgrades in the first place. As mentioned, this analysis makes concrete the links between vague statements about safety culture and the events leading to the accident. In the ECF diagrams of Technical Report A there were contributory factors denoting assumptions that there were 'problems in the safety culture' and in 'safety management'. These might now be replaced by cutting and pasting the more detailed analysis of Figure B-1 into their place in the previous diagrams.

Finally, Figure B-1 shows the complex links between Safety Management issues and the decisions that left a single controller 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.

Additional Recommendation 11:
One of the great benefits of being supported and encouraged in this project has been to trace in detail the mechanisms by which national and international guidelines of Safety Culture and Safety Management Systems have a direct impact upon safety. Very often these guidelines can be criticised as 'too generic', 'irrelevent to current operating priorities' or not specific enough. The analysis presented in this report has shown the direct relationship between problems in the implementation of the company's Safety Policy and the events leading to the accident. It is important that other Air Traffic Management organisations in general, and Safety Managers in particular, are made aware of this direct connection. There is a danger that this aspect of the accident will be ignored or not given due attention given the amount of coverage that has been devoted to the interaction between the controller, the crews and ACAS/TCAS. These issues are important but are arguably less significant for long term safety than the lessons Überlingen provides about the importance of Safety Management Systems.

Comparison with International Guidelines on Safety Management Systems

An analysis of the role that safety management systems might have played in the Überlingen accident is a significant topic. It is the focus of a complementary project also being funded by EUROCONTROL. The following pages, therefore, only provide an initial overview of this complex topic. In particular, they focus on the relationship between the existing guidance on safety management systems and the challenges that faced the national ATM service provider prior to the Überlingen accident. It is important to avoid hindsight bias when reading these various documents. It does not strictly follow that the service provide was violating all elements of the existing guidance simply because an accident occurred. **Nor is it certain that other national service providers are successfully following this guidance because they have avoided a major accident in recent years.**

ESARR3:
The EUROCONTROL guidance on the implementation of Safety Management Systems is contained in the ESARR3 document 'Use of Safety Management Systems by ATM Service Providers'[1]. This document was first made available during July of 2000. The provisions of the requirement were to come into force within three years of its adoption by the EUROCONTROL Commission. However, it seems likely that this was one of the documents that the ATM service provider referred to when issuing the Safety Policy that is cited in the BFU report. For example, ESSAR3 refers explicitly to the 'Safety Policy' that must be drafted by member states, this is the same term referred to in the BFU analysis.

The relevance of ESARR3 to our investigation of the Überlingen accident is apparent from almost the first paragraph; "Safety management is that function of service provision, which ensures that all safety risks have been identified, assessed and satisfactorily mitigated. A formal and systematic approach to safety management will maximise safety benefits in a visible and traceable way." (ESARR3, page 9). Figure B-1 and the previous analysis in Technical Report A have placed a failure in risk assessment at the center of our interpretation of the causes that led to this accident. Similarly, section 5.2.4 of ESARR3 includes a requirement that risk managers "shall ensure that changes to the ATM system are assessed for their safety significance" (ESARR3, page 11).

ESARR3 also provides objectives for the investigation of safety-related occurrences, such as the AIRPROX events that happened in Zurich ACC during Single Man Operating Procedures prior to this accident. Safety managers "shall ensure that ATM operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken" (ESARR3, page 12). The implications of this requirement for the events surrounding the Überlingen accident are less clear. The ATM service provide could argue that they had thoroughly investigated the incidents and approved the continued operation of Single Man Operating Procedures on the basis of current international practice. Similarly, these procedures were not applicable to night operation nor were their technical requirements satisfied by the conditions facing the controllers. For example, these procedures assumed that controllers were equipped with automatic radar target to flight plan correlation which as we have seen was not available in the backup mode of operation used during the SYCO upgrade.

There is a series of further EUROCONTROL documents that is relevant to this accident. For instance, EAM3/GUI1 contains 'ESARR3 Guidance to ATM Safety Regulators'[2]. As might be expected, this again stresses a risk-based approach to the analysis of any significant changes in the operating infrastructure or procedures before those changes are approved. For example, these issues are addressed several times on pages 23 and 24 of the EAM3/GUI1 guidance. There are, however, some areas where our analysis suggests that additional guidance may be of benefit. For instance, on page 24 of this

[1] http://www.eurocontrol.int/src/gallery/content/public/documents/deliverables/esarr3v10ri.pdf
[2] http://www.eurocontrol.int/src/gallery/content/public/documents/deliverables/esarr3_awareness_package/eam3gui1e10ri.pdf

document there is a paragraph which argues that "Since equipment, people and procedures form systems where different levels or sub-systems can be identified; system levels to be addressed should be identified by taking into account combinations of equipment, people and procedures, which may have an impact on the operation". These comments accurately reflect our analysis of the interaction between safety management issues, technical problems in the support offered by the fall-back mode of operation for Single Man Operation and the human factors issues surrounding the simultaneous control of the B757, the A320 and the TU154M from two different workstations. However, the guidance document provides less insight into how ATM service providers might conduct such a layered approach to risk analysis. Consequently, one cannot be certain that this accident would have been prevented even if the ATM service provider had conducted a fully resourced risk assessment of the SYCO upgrade. ESARR4 provides useful guidance but not a fully worked out example on this scale.

Additional Recommendation 12:

It seems clear that the requirements for the implementation of Safety Management Systems, such as those presented in ESARR 3, are well considered and would have played an important role in either preventing or mitigating the conditions that faced the controller during the Überlingen accident. It is less clear what role national or international organisations can play to encourage the monitoring of these requirements. The publication of European Safety Maturity indicators seems a key tool in this process. However, it may be necessary to make the identities of the nations in each level public possibly through a body that is in some way independent of EUROCONTROL to provide the necessary incentives to national regulators.

Additional Recommendation 13:

The international requirements for a risk-based approach to Safety Management Systems often contain accurate and perceptive statements about the need to consider the interaction between systems (people, technology, environmental factors) at different 'layers' of complexity. However, there is little guidance available to Safety Managers on how to do this for a situation that is as complex as that facing the ATM managers during the Überlingen accident.

Transport Canada's Implementation Plan for Safety Management Systems:
Transport Canada has for several years been working on the development of Safety Management Systems as a means of improving the safety of civil aviation. It has recently published a new blueprint for the development and introduction of these systems. The blueprint is supported with considerable additional resources and guidance material hence it forms a useful point of comparison with the information and recommendations in the EUROCONTROL documentation. In particular, there is an extensive web based reference library[3]. The tone and scope is very similar to material presented in ESARR3. For example, similar terms are used to refer to organizations' 'Safety Policy' and the importance of direct feedback through accident and incident reporting. It also includes a series of practical resources on 'Risk Management and Decision Making in Civil Aviation' that are similar to and might also complement material in ESARR4.

There are, however, important cosmetic differences. For instance, TP13881E – Safety Management Systems for Flight Operations And Aircraft Maintenance Organizations – A guide to implementation, contains two sections that distinguish between reactive and proactive approaches to Safety Management. Our analysis of the Überlingen incident confirms the usefulness of this distinction given that we have identified two distinct risk assessment problems. The first is the failure to anticipate the hazards associated with the planned upgrade of the SYCO system. Clearly, this requires a form of proactive safety management where key personnel have to anticipate the future risks associated with a planned action. Our analysis of the Überlingen accident also illustrates some of the problems associated with reactive risk assessment with reference to the two previous AIRPROX incidents. Here the ACC Zurich failed to use valuable information about previous adverse events to predict that there may be future related problems in similar circumstances.

As with the guidance cited in previous sections, it is possible to identify a number of problems with the Transport Canada guidance from our analysis of the Überlingen accident. For instance, the TP13881E documentation argues that "Understanding the hazards and inherent risks associated with everyday activities allows the organization to minimize unsafe acts and respond proactively, by improving the processes, conditions and other systemic issues that lead to unsafe acts. These include - training, budgeting, procedures, planning, marketing and other organizational factors that are known to play a role in many systems-based accidents. In this way, safety management becomes a core-business function and is not just an adjunct management task. It is a vital step in the transition from a reactive culture - one in which the organization reacts to an event, to a proactive culture, in which the organization actively seeks to address systemic safety issues before they result in an active failure". These are important and valuable observations. However, it is unclear how practically they could have been applied to address the specific organisational issues facing the ATM service provide in the months and weeks leading to this accident. There is strong evidence that the service provider did treat safety management as a significant issue, arguably it did not have the central role suggested in the previous citation given the staffing issues and the delays in establishing the Centre of Competence. However, such generic guidance is a long way from the detailed regulatory or advisory support that might have helped the service provider respond to the staff shortages and skill 'gap' that prevented them from realising their well designed Safety Plan.

Additional Recommendation 14:

An approved list of documentation techniques should be established for reactive incident analysis. These need not be 'heavy weight', for example, Transport Canada advocates the MEDA/PEAT tools developed by Boeing. These are little more than mnemonics for the range of causal factors that need to be considered during the analysis of an incident together with some guidance on how to determine the likelihood of any future recurrence.

[3] http://www.tc.gc.ca/CivilAviation/SMS/guidance.htm

Additional Recommendation 15:

Consideration should be given to the development of pathological 'what if' scenarios to support proactive risk assessment. The Überlingen accident and similar ATM incidents have taught us that it can be very difficult to anticipate the complex combinations of human 'error', technical 'failure' and environment conditions that lead to major loss of life. It is possible that short descriptions of previous incidents or some similar technique might be used to encourage Safety Managers to identify the plausible worst case before approving changes in ATM processes.

US Federal Aviation Administration's System Safety Management Programme:
The US FAA have revised their System Safety Management program within the last week (December 2004)[4]. The aim of this programme is to define "the scope purpose, objectives, and planned activities of the Federal Aviation Administration's (FAA) system safety effort as it applies to the safety management for all systems, new and old, providing air traffic control (ATC) and navigation services in the National Airspace System (NAS) as well as the acquisition of systems in support of NAS modernization. The System Safety Management program embodies the FAA's safety culture…It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters". There are many reasons for considering the Überlingen accident in the context of this FAA program. As can be seen from the previous quotation it is pitched at a slightly different level to the Transportation Canada and EUROCONTROL guidance. The FAA are establishing higher level objectives for the national airspace system rather than providing guidance for operating companies, as is the case with Transport Canada, or for a group of national ATM service providers, as is the case with ESARR3. Hence the FAA document has more in common with the Safety Policy that guides an individual national service provider.

The previous quotation from the FAA's System Safety Management program also emphasises its key concern with the modernisation of US airspace. This is again significant given that the update to the SYCO system lies at the heart of the Überlingen accident. However, the actual content of the guidance on safety management is very similar to the material described in the previous documents. For instance, the FAA advocate documented risk assessment prior to any major safety-related interventions in the national airspace systems. This risk assessment must consist of a number of predetermine activities:

1. Implement safety risk management by performing risk assessment and analysis and using the results to make decisions
2. Plan – the risk assessment and analysis must be predetermined, documented in a plan which must include the criteria for acceptable risk
3. Hazard identification – the hazard analyses and assessments required in the plan must identify the safety risks associated with the system or operations under evaluation
4. Analysis – the risks must be characterized in terms of severity of consequence and likelihood of occurrence
5. Risk Assessment – the risk assessment of the hazards examined must be compared to the acceptability criteria specified in the plan and the results provided in a manner and method easily adapted for decisionmaking
6. Decision – the risk management decision must include the safety risk assessment and the risk assessments may be used to compare and contrast options.

This FAA guidance makes a number of key points about the role of risk assessment within Safety Management Systems. Within the context of the Ueberlinger accident arguably the most important of these is that the risk management decision must be used to compare and contrast options. Throughout this analysis of the BFU report and supporting documentation the authors have this report have wondered whether there were any alternate, phased implementation techniques that might have avoided the need to disrupt so many core systems at the same time during a night shift. The accident investigation team provide no clues about this. The absence of such information may provide further evidence of the BFU's focus on the interaction between the flight crew, ACAS/TCAS and the controller's descent commands rather than on the risk assessment processes that might have averted this incident in the first place. The lack of information about alternative update programmes for the SYCO system may also arguably indicate the ATM service provider's failure to conduct any formal risk assessment prior to beginning the maintenance procedure.

[4] http://fast.faa.gov/toolsets/SafMgmt/section1.htm

As mentioned, a sustained analysis of national and international guidance on Safety Management Systems in relation to the Überlingen accident is a complex and substantial topic that can only be summarised in this report. However, an initial analysis of the extensive and new FAA guidance reveals a number of other important points. In particular, they identify a number of phases during the planning of maintenance and development activities when risk assessments should be conducted. The obvious advice is that it should be performed as early as possible in the planning of operations such as the change to sectorisation in ACC Zurich. However, the FAA guidance also identified other triggers. For example, incident reports can trigger a reassessment of previous risk assessments if they provide key information about potential hazards that had not previously been anticipated. Similarly, the use of sub-contracting or of other changes in the operating environment might also force the maintenance of a documented risk assessment. In the Überlingen accident, the previous AIRPROX incidents should have triggered a sustained analysis of the Single Man Operating Procedures. The FAA guidance points out, however, that this should ideally have been a revision of a *risk assessment that should ideally have already been performed before any of these procedures had been approved.*

Additional Recommendation 16:

Consideration should be given to the publishing guidance on how to use risk assessment as a tool to critically analyse competing options rather than simply to validate a single planned procedure. The FAA are correct in recognising the value of this comparative approach to decision making where different risks are assessed rather. There is a danger that risk assessments will be tailored to demonstrate the acceptability of 'single option' decisions.

Additional Recommendation 17:

The Überlingen accident shows that incidents, such as the Zurich AIRPROX reports during Single Man Operating Procedures, should act as triggers to formal risk assessment within the guidelines associated with a Safety Management System. However, the FAA's recent focus on system-wide risk assessment may argue against this approach. If we wait for incidents to trigger risk assessments or if we wait for system upgrades to force new hazard analysis then there will be large areas of our airspace systems that have no formal risk assessment. It may, therefore, be necessary for ATM service providers to increase the scope of their Safety Management Systems to proactively create a more coherent Safety Case similar to the prototype arguments being produced by EUROCONTROL for the implementation of RVSM etc.

Conclusions

This is the second report of two issued under this contract. The first report identified recommendations in the BFU report that were not fully supported by their causal analysis. The first report also used an Events and Causal Factors analysis to identify eight additional recommendations from the BFU report. The principle insight from all of this work was that the BFU did good work in analysing the role of ACAS/TCAS in the two planes. However, less attention was paid to the inadequate risk assessments that exposed the controllers to extreme operational demands during the SYCO systems upgrade. This report builds on the findings of the initial document. In particular, it goes on to look at the role that Safety Management Systems played in the accident. We concur with the BFU that the Swiss authorities had well-documented procedures and principles that would encourage the development of a sound Safety Management System. These principles were in accordance with ICAO and EUROCONTROL guidelines. However, the Swiss ATM organisations lacked the experience and the personnel to implement those procedures. Partly as a result of this opportunities were missed to learn from two AIRPROX incidents that had similarities to the events before the Überlingen accident.

It is important to stress that we have focussed on the controllers' perspective in this report. The role of both crews and the impact of ACAS/TCAS have already been well covered by the BFU. It is also important to stress that this report is not intended to be a criticism of the BFU report. They conducted a thorough and detailed investigation under difficult circumstances and their recommendations have clearly made a significant contribution to aviation safety. However, our aim has been to go beyond the existing recommendations and extract any additional lessons that might be learned from this very unfortunate incident. Our secondary aim has also been to ensure that the recommendations made by the BFU were supported by either systemic or immediate causes.

Summary of Findings:
As mentioned, our analysis confirms the BFU's insight that the ATM service provider had an appropriate Safety Policy at the time of the accident. However, there were a number of resource and organisatiojnal problems that prevented them from implementing the policy in a satisfactory manner. The BFU report identified a number of problems that frustrated the operation of the Safety Management Systems: there were delays in Establish a Centre of Competence; this delay was partly related to staffing shortages; these shortages also prevented adequate ATCO training and advanced training in 'emergency' situations; there were also inadequate night staffing levels and single man operating procedures; on reason for this was that there were problems in the internal reporting of safety incidents such as two previous AIRPROXs in ACC Zurich.

Our analysis has extended that of the BFU by showing in a concrete way how these different problems interacted and created the context in which the Überlingen accident was likely to occur. Figure B-1 related high level observations about the safety culture and safety management systems to very specific events in the accident. It is important the ATM officers and Safety Managers see these connections if they are to realise the true importance of Safety Management Systems in the prevention of future accidents or near-miss incidents.

In addition, our analysis has identified the following additional recommendations:

Additional Recommendation 9: The Überlingen accident was caused by failures in the safety management systems that did not ensure the use of appropriate risk assessment techniques prior to the SYCO upgrade. Appropriate procedures and principles were in place within Swiss Air Traffic Management and it seems clear that had these been followed then the controllers might not have been exposed to such demanding operating conditions. It follows that EUROCONTROL and the ICAO

might, therefore, usefully provide additional services in helping organisations implement these good practices and where appropriate might assist national regulators in monitoring their implementation.

Additional Recommendation 10: The Überlingen accident was pre-dated by two AIRPROX incidents in Zurich ACC that eloquently illustrated the dangers of Single Man Operating Procedures even under more benign circumstances that existed on the night of the accident. EUROCONTOL ESSAR guidelines require that such incidents should normally trigger a formal risk assessment and yet this was not done in either of these cases. It is difficult to be certain about why the guidelines were not followed here. The BFU report does not contain enough detail and this issue certainly merits further investigation. These AIRPROX incidents represent valuable learning opportunities that were missed *before* the Überlingen accident.

Additional Recommendation 11: One of the great benefits of being supported and encouraged in this project has been to trace in detail the mechanisms by which national and international guidelines of Safety Culture and Safety Management Systems have a direct impact upon safety. Very often these guidelines can be criticised as 'too generic', 'irrelevent to current operating priorities' or not specific enough. The analysis presented in this report has shown the direct relationship between problems in the implementation of the company's Safety Policy and the events leading to the accident. It is important that other Air Traffic Management organisations in general, and Safety Managers in particular, are made aware of this direct connection. There is a danger that this aspect of the accident will be ignored or not given due attention given the amount of coverage that has been devoted to the interaction between the controller, the crews and ACAS/TCAS. These issues are important but are arguably less significant for long term safety than the lessons Überlingen provides about the importance of Safety Management Systems.

Additional Recommendation 12: It seems clear that the requirements for the implementation of Safety Management Systems, such as those presented in ESARR 3, are well considered and would have played an important role in either preventing or mitigating the conditions that faced the controller during the Überlingen accident. It is less clear what role national or international organisations can play to encourage the monitoring of these requirements. The publication of European Safety Maturity indicators seems a key tool in this process. However, it may be necessary to make the identities of the nations in each level public possibly through a body that is in some way independent of EUROCONTROL to provide the necessary incentives to national regulators.

Additional Recommendation 13: The international requirements for a risk-based approach to Safety Management Systems often contain accurate and perceptive statements about the need to consider the interaction between systems (people, technology, environmental factors) at different 'layers' of complexity. However, there is little guidance available to Safety Managers on how to do this for a situation that is as complex as that facing the ATM managers during the Überlingen accident.

Additional Recommendation 14: An approved list of documentation techniques should be established for reactive incident analysis. These need not be 'heavy weight', for example, Transport Canada advocates the MEDA/PEAT tools developed by Boeing. These are little more than mnemonics for the range of causal factors that need to be considered during the analysis of an incident together with some guidance on how to determine the likelihood of any future recurrence.

Additional Recommendation 15: Consideration should be given to the development of pathological 'what if' scenarios to support proactive risk assessment. The Überlingen accident and similar ATM incidents have taught us that it can be very difficult to anticipate the complex combinations of human 'error', technical 'failure' and environment conditions that lead to major loss of life. It is possible that short descriptions of previous incidents or some similar technique might be used to encourage Safety Managers to identify the plausible worst case before approving changes in ATM processes.

Additional Recommendation 16: Consideration should be given to the publishing guidance on how to use risk assessment as a tool to critically analyse competing options rather than simply to validate a single planned procedure. The FAA are correct in recognising the value of this comparative approach to decision making where different risks are assessed rather. There is a danger that risk assessments will be tailored to demonstrate the acceptability of 'single option' decisions.

Additional Recommendation 17: The Überlingen accident shows that incidents, such as the Zurich AIRPROX reports during Single Man Operating Procedures, should act as triggers to formal risk assessment within the guidelines associated with a Safety Management System. However, the FAA's recent focus on system-wide risk assessment may argue against this approach. If we wait for incidents to trigger risk assessments or if we wait for system upgrades to force new hazard analysis then there will be large areas of our airspace systems that have no formal risk assessment. It may, therefore, be necessary for ATM service providers to increase the scope of their Safety Management Systems to proactively create a more coherent Safety Case similar to the prototype arguments being produced by EUROCONTROL for the implementation of RVSM etc.