A STAMP Model of the Überlingen Aircraft Collision Accident

by

Brian Wong

S.B. Aerospace Engineering with Information Technology
Massachusetts Institute of Technology, 2003

Submitted to the Department of Aeronautics and Astronautics
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Aeronautics and Astronautics

at the

Massachusetts Institute of Technology

September 2004

© 2004 Massachusetts Institute of Technology
All rights reserved

Signature of Author .............................................................

Department of Aeronautics and Astronautics
August 6, 2004

Certified by ......

Nancy Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by ..........................................

Jaime Peraire
Professor of Aeronautics and Astronautics
Chair, Committee on Graduate Students
A STAMP Model of the Überlingen Aircraft Collision Accident

by

Brian Wong

Submitted to the Department of Aeronautics and Astronautics
On August 6, 2004 in Partial Fulfillment of the
Requirements for the Degree of Master of Science in
Aeronautics and Astronautics

ABSTRACT

STAMP is a method for evaluating accidents that is based on systems theory. It departs from traditional event chain models that tend to focus on human errors instead of the goals and motives that triggered the errors. The thesis presents a STAMP model of the mid-air collision that occurred on July 1, 2002 near Überlingen, Germany. This model focuses on the air traffic controller in charge of the aircraft that collided and the surrounding central environment at ACC Zurich, which was the ATC center controlling the aircraft at the time. First the components in the system are analyzed to determine their roles in the system and to identify the safety-related issues. Next, the interactions of the components and the resulting communications failure are studied. Conclusions as to the causes of the accident are presented. A system dynamics model of the control room environment is constructed and studied to determine how the issues relating to the accident developed over time. Finally, the findings from the STAMP model are summarized and recommendations are made based on the analysis. The recommendations based on the model agree with those of the official accident investigation report; in addition, several new recommendations are made.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics
Acknowledgements

I would like to thank:

- Prof. Nancy Leveson, my thesis advisor, for her guidance and for employing me for the past year.

- My lab mates from the various labs housed in 33-407 for their help with my research and course work, and for making my graduate school experience a good one. I would especially like to thank Karen Marais for her mentorship.

- My professors and the administrative staff at MIT for all their help and guidance throughout the past few years.

- My fellow students in the MIT Aero/Astro Department for all the good times and the bad times.

- My family and friends for everything else.

That is all.
Table of Contents

1 Introduction .................................................................................................................. 13
   1.1 Motivation: STAMP ............................................................................................... 13
   1.2 Motivation: Überlingen Aircraft Collision Accident ........................................... 13
   1.3 Thesis Framework ................................................................................................. 14

2 Background ............................................................................................................... 15
   2.1 Background: Accidents and STAMP ...................................................................... 15
   2.2 Background: Überlingen Aircraft Collision Accident ......................................... 17

3 Application of STAMP Model to Accident ........................................................... 19
   3.1 System Components ............................................................................................. 19
      3.1.1 Controller on Duty at ACC Zurich ............................................................... 20
      3.1.2 TU154M Crew ............................................................................................... 24
      3.1.3 B757-200 Crew .............................................................................................. 26
      3.1.4 Skyguide Management .................................................................................. 28
      3.1.5 ACC Zurich .................................................................................................... 30
      3.1.6 Skyguide Center of Competence (CoC) ......................................................... 33
      3.1.7 Supervisor who Briefed the Controllers at 21:00 hrs After his Shift ............... 34
      3.1.8 Departing System Manager ........................................................................... 34
      3.1.9 Bulletin Board Containing Directives Regarding Technical Work ................. 35
      3.1.10 ACAS/TCAS ................................................................................................. 35
      3.1.11 Flight Operators ........................................................................................... 36
      3.1.12 Controller at UAC Karlsruhe ....................................................................... 37
      3.1.13 Controller at ACC Munich ............................................................................ 37
      3.1.14 System Manager and ATC Technical Expert Assisting Sectorization Work Technicians .......................................................... 38
      3.1.15 Technical Expert Assigned to Assist Controllers During the Sectorization Work .......................................................... 39
      3.1.16 Controller Assistant Aiding the Controller ..................................................... 39
      3.1.17 SWI-02 & Bypass Telephone Systems .......................................................... 40
      3.1.18 Optical STCA ............................................................................................... 40
      3.1.19 Aural STCA ................................................................................................ 41
      3.1.20 Summary of Individual Component Analysis ............................................... 42

7
3.2 Component Interactions ................................................................. 43
  3.2.1 Communications breakdown on the night of the accident ......... 48

4 A System Dynamics Model of the Control Room Environment at ACC Zurich .................................................................................................. 49
  4.1 The Practice of Having Only One Controller on Active Duty During the Night Shift ................................................................. 51
  4.2 Staff Training and Experience ...................................................... 52
  4.3 Unclear and Incomplete Directives ............................................. 54
  4.4 Controller Assistants’ Perception of Controllers’ Attitudes .......... 56
  4.5 Sectorization Work and Risk Management to Limit its Impact ....... 57
  4.6 Dependencies that Develop Over Time ....................................... 59
  4.7 Conclusion to Analysis Using the System Dynamics Model .......... 59

5 Summary and Recommendations ......................................................... 61
  5.1 The Practice of Having Only One Controller on Active Duty During the Night Shift ................................................................. 61
  5.2 Insufficient Training and Refresher Training for Emergency Situations, Automation, Team Resource Management and Human Factors ........... 62
  5.3 Unclear and Incomplete Directives ............................................. 62
  5.4 Controller Assistants’ Perception of Controllers’ Attitudes .......... 63
  5.5 ACAS/TCAS Regulations and Operational Procedures, and Flight Crew Training ................................................................. 63
  5.6 Sectorization Work and Risk Management to Limit its Impact ....... 64
  5.7 Dependencies on Automation that Develop Over Time ............... 65
  5.8 Other Recommendations ............................................................. 66
  5.9 Conclusion ..................................................................................... 67

References ............................................................................................ 69
List of Figures

Figure 1: Components Surrounding the Controller at ACC Zurich......................... 44
Figure 2: Links Degraded Due to Poor or Unsafe Practices........................................ 44
Figure 3: Links Lost Due to Sectorization Work..................................................... 46
Figure 4: Links Lost Due to Unusual Situations...................................................... 46
Figure 5: Links Effectively Lost Due to the Controller Being Unaware of their Existence.. 47
Figure 6: A System Dynamics Model of the Control Room Environment at ACC Zurich
During the Night Shift............................................................................................ 50
Figure 7: Variables Related to the Practice of Having Only One Controller on Active
Duty During the Night Shift .................................................................................. 51
Figure 8: Variables Associated with Insufficient Training......................................... 53
Figure 9: Variables Relating to Directives about the Planned Sectorization Work........ 55
Figure 10: Variables Related to Controller Assistants' Perception of Controllers' Attitudes
Towards Them ....................................................................................................... 57
Figure 11: Variables Affected By Sectorization Work and Risk Management.............. 58
List of Abbreviations

ACAS  Airborne Collision Avoidance System
ACC   Area Control Center
ATC   Air Traffic Control
BAZL  Bundesamt für Zivilluftfahrt
BFU   Bundesstelle für Flugunfalluntersuchung (German Federal Bureau of Aircraft Accidents Investigation)
CA    Controller Assistant
CoC   Center of Competence (Responsible for the functions of safety, quality, audit and risk management within Skyguide)
ICAO  International Civil Aviation Organization
PF    Pilot Flying
PIC   Pilot In Command
PNF   Pilot Not Flying
RA    Resolution Advisory
SMOP  Single Manned Operation Procedures
STCA  Short Term Conflict Alert
TA    Traffic Advisory
TCAS  Traffic Alert and Collision Avoidance System
TRM   Team Resource Management
UAC   Upper Area Control
1 Introduction

1.1 Motivation: STAMP

STAMP (Systems Theoretic Accident Model and Processes) is a method for evaluating accidents that departs from traditional event chain accident models. Event chain models tend to focus on human errors instead of the goals and motives that triggered the errors. STAMP is based on the principles of systems theory and therefore has the advantage of being able to account for social and organizational factors. It is a more flexible approach that allows modern systems to be described as a set of interrelated components connected in dynamic equilibrium by constraints and feedback control loops.

A STAMP model is an effective tool for modeling aircraft accidents as it provides a holistic view allowing occurrences to be traced back to systemic failures and problems at the organizational level instead of individual events and decisions. A STAMP model also attempts to explain how and why safety constraints and the interactions between different elements in the system degraded over time to create the conditions necessary to facilitate an accident.

1.2 Motivation: Überlingen Aircraft Collision Accident

The Überlingen Aircraft Collision Accident is an example of a serious mid-air collision that occurred during a period of low traffic. Its occurrence illustrates a failure of the primary role of the air traffic control system, which is to maintain separation between aircraft, even without the system being in a fully saturated state. It is the seriousness of this accident and the ordinary circumstances under which it occurred that makes it an interesting case to study.

By applying the STAMP model to the Überlingen Aircraft Collision Accident, this thesis hopes to illustrate the use of STAMP in determining what systemic failures contributed to the accident.
1.3 Thesis Framework

This thesis first introduces background information on STAMP and the Überlingen Aircraft Collision Accident. It then uses the principles of STAMP to discuss and analyze the different components involved in the accident. These components include people involved in the events leading up to the accident such as the flight crews of the two aircraft and the people in the control room at ACC Zurich, which was the air traffic control center that was controlling the aircraft at the time of the accident. The components also include automated systems as well as entities such as regulatory authorities. For the purposes of illustration, this thesis will only look at the components centered on the controller at ACC Zurich. Note that in no way does this imply that the controller was responsible for the accident. The analysis here has been focused based on the information available to the author and other constraints. A full STAMP analysis would look at the entire system including components centered on the aircraft and the organizational structure of the Swiss air navigation services.

Included in the discussion and analysis will be a look at the interactions among the different components in the system, and the communications breakdown that resulted. Using this discussion and analysis, conclusions will be drawn regarding the causes of the accident. These causes will be compared to those from the official investigation report published by the German Federal Bureau of Aircraft Accidents Investigation (BFU).

Next, a system dynamics model will be constructed that illustrates the variables in play in the control room at ACC Zurich. Note again that this is only a portion of the full model of the system. For a full and complete model, other sub-models that look at related aspects such as the safety culture at Skyguide and regulatory agencies involved in developing guidelines for TCAS would also be explored. The control room environment at ACC Zurich was chosen for this thesis based on the information available and the author’s background. Conclusions will be drawn from this model that will be compared with the causes of the accident found by the BFU. A summary will be presented of the findings of the STAMP model and how they compare to the findings from the official investigation report. Recommendations based on the STAMP model will be compared to the BFU’s recommendations. The advantages of using a STAMP model and suggestions for future work will also be presented.
2 Background

This section gives a brief overview of accidents and STAMP, followed by information on the Überlingen Aircraft Collision Accident. Additional information on both STAMP and the Überlingen Accident may be found in the references.

2.1 Background: Accidents and STAMP

Why do accidents occur? Traditionally, the answer to this question is that a series of extraordinary events happen that are often blamed on human operator error. However, what these traditional accident models fail to look at is why the human performed the action, and what were the causes for that behavior.

In a systems-centric view, accidents occur because the behaviors of a number of components in the system interact in a way to produce unsafe conditions. It is important to note that the behavior of each component on its own is not necessarily unsafe, but the dysfunctional interactions between components can cause or increase the potential for accidents. The fact that each individual behavior is not unsafe on its own is the reason why regular safety checks often fail to notice any problems in the system. Usually when the system is initially designed, the interactions between different components do not immediately generate unsafe conditions. Why then do these unsafe conditions eventually occur? One answer is that, over time, the different components in the system evolve and adapt to changes in the environment and to upgrades. As a result they may end up interacting in ways that were not possible in the original design, leading to the inability of previously adequate safety constraints to effectively prevent unsafe conditions from occurring.

Given this information, one would imagine that when upgrading a subsystem of a larger system, a thorough study of the effects of the upgrade would be conducted. The problem arises when the study overlooks effects that occur in other subsystems that seem to only be remotely connected to the subsystem being upgraded, or if the study does not account
for dynamic effects that only become apparent after a certain period of time. A good case of an asynchronous subsystem upgrade that was tested to be perfectly safe on its own, but triggered an unsafe condition when it interacted with another subsystem, can be found in the now infamous Ariane 5 rocket example [Leveson 2004b]. Perfectly good legacy software from the Ariane 4 rocket was combined with perfectly good new software written for the Ariane 5. Although both subsystems worked fine on their own for the environments for which they were designed, the legacy software from the Ariane 4 was displaced from its usual environment causing a change in behavior, and the interaction of the two caused an unsafe condition to occur. This example and numerous others illustrate how individual safety analysis of two separate components fails to take into account changes in behavior that occur when a change of environment occurs. The systems theoretic view of accidents attempts to model a system in such a way that allows the static and dynamic interactions among different components over time to be brought to the foreground for analysis of unsafe combinations.

STAMP is a systems theoretic view of accidents that captures these otherwise hidden interactions. The main concepts contained in STAMP are those of safety constraints, control loops and process models, and socio-technical levels of control. Viewing a system in these terms, accident factors are classified in the following categories:

1. Inadequate enforcement of safety constraints due to:
   a. Inadequate control algorithms
   b. Inconsistent process models
   c. Inadequate coordination among controllers and decision makers
2. Inadequate execution of control actions
3. Inadequate or missing feedback

Using STAMP's systemic view to study accidents enables the root causes in the system to be identified and corrected to create a better and safer system. More detailed information on STAMP may be obtained from [Leveson 2004a] and [Leveson et al. 2004].
2.2 Background: Überlingen Aircraft Collision Accident

On the night of July 1, 2002, a midair collision occurred between two mid-sized jet aircraft: a Tupolev TU154M en route from Moscow, Russia to Barcelona, Spain and a Boeing B757-200 en route from Bergamo, Italy to Brussels, Belgium. The collision occurred north of the city of Überlingen, Germany in airspace controlled by ACC Zurich in Switzerland, and resulted in complete haul loss of both aircraft and the fatality of all 71 people on board including 60 children. The Tupolev TU154M suffered an in-flight break-up. The Boeing 757-200 lost most of its vertical tail in the collision and was destroyed by ground impact forces following loss of control.

Since the accident occurred over Germany, the Bundesstelle für Flugunfalluntersuchung (BFU), or German Federal Bureau of Aircraft Accidents Investigation, was in charge of the official accident investigation. Many of the facts in this thesis are derived from the BFU’s English translation of the official German Investigation Report published by the BFU in May 2004 [BFU 2004]. Additional information was obtained from documents published by Skyguide, the Swiss air navigation service company that was in charge of the airspace in which the accident occurred. The bibliography contains a detailed list of references.

The BFU accident report determined that the following were immediate causes of the accident:

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."

2. "The TU154M crews followed the ATC instruction to descend and continued to do so even after TCAS advised them to climb. This maneuver was performed contrary to the generated TCAS RA."
The BFU accident report determined that the following were systemic causes of the accident:

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 standardized, incomplete and partially contradictory.

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.

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."
3 Application of STAMP Model to Accident

Using STAMP, the behavior of each of the subsystems in the system can be modeled to gain insight into the accident causes. What follows is an example that centers on the air traffic controller at ACC Zurich responsible for the two aircraft at the time of the accident. Note that this choice is not intended to imply that the controller was at fault in the accident. Other models of subsystems could focus on the flight crews and their training, the aircraft involved, or other components. The first part of the analysis will focus on the static system that existed on the night of the accident.

3.1 System Components

The following elements that make up the portion of the system surrounding the controller at ACC Zurich will be discussed.

1. Controller on Duty at ACC Zurich
2. TU154M Crew
3. B757-200 Crew
4. Skyguide Management
5. ACC Zurich
6. Skyguide Center of Competence (CoC)
7. Supervisor who Briefed the Controllers at 21:00 hrs After his Shift
8. Departing System Manager
10. ACAS/TCAS
11. Flight Operators
12. Controller at UAC Karlsruhe
13. Controller at ACC Munich
14. System Manager and ATC Technical Expert Assisting Sectorization Work Technicians
15. Technical Expert Assigned to Assist Controllers During the Sectorization Work
16. Controller Assistant Aiding the Controller
17. SWI-02 & Bypass Telephone Systems
18. Optical STCA
19. Aural STCA
These elements of the model will be explored further in the following sections. Each component will be described in terms of the following behavioral aspects:

1. Safety requirements and constraints
2. Context in which decisions are made
3. Inadequate control actions
4. Mental model flaws
5. Coordination

By analyzing these aspects of each component, insight can be obtained as to the role of each component in the system and what could have been done to prevent the occurrence of the accident. Note that for some components, not all five aspects listed above apply. For example, an inanimate component in the system such as TCAS is not capable of conscious thought and therefore the second and fourth items above do not apply.

3.1.1 Controller on Duty at ACC Zurich

The controller on duty at ACC Zurich at the time of the accident was known by his colleagues and supervisors to be a competent and knowledgeable controller, and had a professional and team-oriented attitude. On his otherwise perfect professional record there was one minor separation infringement incident from May 2001. The incident involved a recognized conflict that was compounded by the lack of a second controller to aid in traffic monitoring.

**Safety requirements and constraints:**

The task of the controller at ACC Zurich was to ensure adequate horizontal and vertical separations between aircraft in the airspace that he was controlling by issuing timely instructions to flight crews. He was also responsible for making sure that the flight crews complied with the instructions.

**Context in which decisions made:**

The controller on duty at ACC Zurich was qualified and licensed in accordance with current regulations, and he was not impaired by medicine, drugs or alcohol at the time of the collision.
The controller on duty was the only one in the control room at the time of the accident. Only two controllers were scheduled to perform the tasks of the radar planning controller and the radar executive controller as well as the tasks of the chief controller and the system manager. In addition, in a practice tolerated by management, during times of low traffic, one controller would retire to the break room while the other controller handled the tasks of both controllers. As a result, one controller was handling multiple tasks that required working from two workstations, of which he could only attend to one at a time. Note that while there was only one controller present in the control room, other staff members were present including a controller assistant whose job it was to aid the controller.

Sectorization work was being done on the night of the accident. As a result, the radar system was being operated in fallback mode and the separation minimum had been increased from 5 to 7 NM. In fallback mode, the MV 9800 radar computer was not available to controllers, meaning that automatic correlation of the flight targets and the optical STCA was not displayed. Normally during situations where only one controller was on duty, these automated systems would provide necessary error checking to detect controller error; however, that error checking was not available as a result of the sectorization work.

A delayed A320 on approach to Friedrichshafen appeared after the control strips for the two aircraft involved in the accident had arrived. At this point, the controller had to assume the three functions of radar planning, radar executive and approach on two adjacent workstations using two different radio frequencies. Had the controllers known about the approaching A320 before one of them retired to the break room, they would probably have both stayed on duty as the ATM Manual ZC requires that one controller give his undivided attention to an aircraft on approach. However, by the time the A320 arrived, the resting controller had already departed and the break room was located too far away for the controller on duty to call the resting one.

The SWI-02 direct phone connections to adjacent ATC units were not available because of sectorization work. The bypass phone system was not available as well from 21:23 hrs
to 21:34:37, or around 12 minutes before to 48 seconds before the accident. By the time
the phone system was available again, the controller was too busy dealing with aircraft to
notice that the phone system was working, and three calls from UAC Karlsruhe and one
call from Friedrichshafen were left unanswered.

Additionally, dealing with the failure of the bypass telephone system connection to
Friedrichshafen partially occupied the controller’s attention as well, delaying him
noticing the imminent separation infringement. The controller was paying more attention
to the A320 than the other two aircraft during the five minutes leading up to the collision.
Had he been completing the tasks of radar planning of checking the actual locations of
the aircraft with the control strips, he would have recognized the impending conflict.

Three airplanes should generally be a safe number of airplanes for one controller to
handle, and therefore the controller on duty did not request additional help from the
controller in the break room. However, the additional problem of the failure of the
bypass telephone system diverted his attention away from the task of maintaining proper
separation. The controller’s repeated attempts to call Friedrichshafen about the
approaching A320 diverted his attention away from the separation task. By the time he
realized that there was a problem with the telephone system, it was too late to ask the
resting controller for help or to delegate the task to the controller assistant who was also
present.

Mental model flaws:

The controller was not fully aware of the technical restrictions on the radar system in
fallback mode. For example, he did not remember that the optical STCA (Short Term
Conflict Alert) was not available in this degraded mode. Although he had been informed
orally about the sectorization work, he had not read the directives regarding the work.
However, the directives did not contain information about the operational effects of the
work either. In addition, the controller had not been informed in advance that the SWI-
02 direct telephone lines to adjacent ATC units would not be available that night.
There were ten technicians scheduled to carry out the planned sectorization work, of which five or six were in the control room. A staff member from ACC Zurich management was acting as a coordinator between controllers and technicians, and a system manager was also on duty. An additional technical expert was also assigned to control the impact of the sectorization work on the operational ATC staff. The controller was not aware of the tasks of these extra staff members and thus he did not realize that he could have asked them for assistance. The controller assumed that the technical expert was just another technician assisting the technicians in interfacing with operational systems. These additional staff members could have helped the controller with the situation, but they did not recognize the urgency of the situation.

The controller considered the separation infringement problem solved too early once he had given instructions to the crew of the TU154M to descend. Being occupied with the A320 on the other frequency at the other workstation, he did not hear the crewmembers of the B757-200 voice their descent action 13 seconds prior to the collision following the TCAS RA they had received.

The controller also had the option of separating the two converging planes earlier; however, he did not do so because he did not think that the A320 task would be lengthened by the phone system problem.

The controller did not know that a TCAS RA had been generated shortly after his instruction to the TU154M that was contrary to it, and that therefore the B757-200 had received a TCAS RA to descend. He did know that the B757-200 had already descended to FL 356 at the time that he issued the instruction to the TU154M to descend as the last radar update indicated that the B757-200 was still at FL 359, a value that was within the tolerances for FL 360. The BFU stated in their recommendations that the frequency of radar update be increased.

**Inadequate control actions:**

As a result of the radar system being in fallback mode, the regular horizontal separation requirement of 5 NM was raised to 7 NM. To ensure this separation, the controller
should have issued an instruction to the TU154M to descend to FL 350 at 21:33:49 hrs at the latest, based on a typical descent rate of 1000 ft/min. Instead, the instruction was not given until at least a minute later. Had this instruction been given in time, the accident would not have occurred and the TCAS TA and RA would not have even been issued. The BFU report on the accident also noted that the controller’s phraseology in the instruction lacked the proper urgency of the situation.

The controller could also have separated the converging planes even earlier once they appeared on his screen; however, he did not exercise this option as he did not feel that the imminent approach was crucial and could be handled later. When the controller returned from dealing with the A320 to focus on the two other airplanes, he immediately recognized the conflict and issued an avoidance instruction to the TU154M crew, which the crew acted on immediately and acknowledged after some delay. The controller was not aware and could not have been aware of the TCAS RA that had been issued after his instruction that was contrary to it because there was no downlink in place to relay TCAS advisories to air traffic controllers. The BFU recommended that TCAS downlinks be installed to inform controllers of TCAS advisories.

3.1.2 TU154M Crew

Safety requirements and constraints:

The TU154M crew was responsible for safely flying their aircraft according to its flight operations manual along a flight plan filed in advance. The crew was responsible for obeying instructions from the controller and warning systems in the cockpit, and permission to deviate from the flight plan needed to be obtained from the controller.

Context in which decisions made:

The crewmembers of the TU154M held the required valid licenses and medical certificates and were not impaired by medicine, drugs or alcohol at the time of the collision.
The commander of the TU154M had identified the potential conflict when the distance between the airplanes was around 10 NM, and so the TCAS TA was not a surprise for the crew. Thus the controller’s instruction to descend to FL 350 to avoid the approaching traffic seemed reasonable. Note that only a TCAS TA had been issued at this point, meaning that the aircraft had not been told to descend or climb to avoid approaching traffic.

The decision to follow the controller’s instruction was made swiftly as the crew was in a situation of uncertainty that could be settled by following that instruction. After the crew received the TCAS RA to climb they continued to follow the controller’s instruction to descend, as it seemed to be the correct action, and this notion was reinforced by the controller’s second instruction to descend. It was also reinforced by information from the controller that the other aircraft was still at FL 360.

**Mental Model Flaws:**

The TU154M crew assumed that the controller had the situation under control since he explicitly instructed them to descend to FL 350 to avoid the approaching traffic. After TCAS issued a climb RA, the crew continued to descend as they assumed, based on the controller’s repeated instruction to descend, that the situation was under control. The correctness of the descend command was also reinforced by the information from the controller that the other aircraft was at FL 360. Unfortunately, the controller and the TU154M crew did not realize that the B757-200 crew had just initiated a descent following the descend RA that they had received from their TCAS unit.

The TU154M crew did not take into account that a TCAS RA involves two complementary instructions. Had this occurred to them, they may have followed the TCAS instruction instead of the controller, or at least questioned the controller’s decision to have them descend. The TU154M crew did not question the controller’s instruction, and the assumption made by the BFU report was that they felt that the controller’s instruction was meant as a maneuver to avoid an imminent collision as opposed to a maneuver to re-establish the prescribed separation.
Inadequate control actions:

The TU154M crew was given contradictory instructions from the controller at ACC Zurich and the TCAS RA. Although the flight operations regulations of the TU154M operator and ICAO documents do not clearly indicate what to do in this scenario, the operator’s regulations did explicitly state that maneuvers in contradiction to a TCAS RA were prohibited. The TU154M crew did not verify the contradiction with the controller, nor did they make any attempt to do so. While the copilot of the TU154M did comment on the contradiction, he was ignored by the pilots as he was riding in the rear of the cockpit and did not have an assigned function on this flight. The lack of clear regulations and the lack of proper TCAS training contributed to the crew disobeying the TCAS RA.

3.1.3 B757-200 Crew

Safety requirements and constraints:

The B757-200 crew was responsible for safely flying their aircraft according to its flight operations manual along a flight plan filed in advance. The crew was responsible for obeying instructions from the controller and warning systems in the cockpit, and permission to deviate from the flight plan needed to be obtained from the controller.

Context in which decisions made:

The crewmembers of the B757-200 held the required valid licenses and medical certificates and were not impaired by medicine, drugs or alcohol at the time of the collision.

The B757-200 crew did not notice the approaching conflicting traffic until the TCAS traffic advisory alerted the commander. This lack of awareness is evidenced by the fact that the first officer, who was flying the aircraft, handed the controls over to the PIC and left to use the lavatory just prior to the TCAS TA. Had the crew noticed the approaching traffic on the VSI/TRA, the first officer would probably not have left at that moment. However, procedures do not require the crew to be constantly observing the TCAS display, and the system is designed to alert the crew using an aural warning. The BFU
report inferred that the first officer was on his way back to his seat when the TA warning sounded.

Between the time when the TCAS RA occurred and the first officer returned to his seat, the PIC had to handle both the tasks of the PF and the PNF. Since reacting to the TCAS RA to descend was the higher priority task, he performed this action first. The next task was to contact the controller at ACC Zurich in regards to his action. Unfortunately, the frequency was occupied by radio communications between the controller and the crew of the TU154M until the time when the first officer returned to his seat. The message about the descent was transmitted soon after.

The BFU thus concluded that the delay between the execution of the descent maneuver and the report to ACC Zurich was due to the unique situation that occurred.

**Mental model flaws:**

When the B757-200 crew finally transmitted to ACC Zurich that they had initiated a descent maneuver in accordance with the TCAS RA, the controller did not acknowledge the message as he was occupied at the other console, attempting to contact Friedrichshafen via the failed telephone system. The crew was not aware that the controller was not paying attention to the impending collision. They incorrectly assumed that everything was under control.

**Inadequate control actions:**

The BFU report concluded that the B757-200 crew reacted to the situation in the correct way and followed the procedures in the best way possible given the unique situation. The analysis here did not find any evidence to the contrary, and the unfortunate chance of the first officer being in the lavatory at the time of the TA was simply a case of being in the wrong place at the wrong time. Yet this situation leads to the additional conclusion that perhaps more safety measurements need to be introduced. An example for this case would be to have an additional warning system to guard against separation infringements that is switched on when only one pilot is left in the cockpit.
3.1.4 Skyguide Management

Safety requirements and constraints:

In accordance with a letter of agreement, ACC Zurich was responsible for air traffic control in the portion of German airspace where the accident occurred. Skyguide, the Swiss air navigation services provider, was responsible for maintaining a strong internal safety culture and for promoting safe practices among its staff members. Skyguide was also responsible for providing training and advanced training for its air traffic control officers.

Context in which decisions made:

At the time of the accident, Skyguide was in the process of correcting weaknesses and deficiencies that had been identified though internal and external audits. Skyguide management had published a new safety policy on October 23, 2001 that was in compliance with ICAO, Eurocontrol and Bundesamt für Zivilluftfahrt (BAZL) requirements including requirements that were not mandatory at the time. According to this policy, a safety culture was to be developed in which managers and employees were aware of their importance to safe operations. At the time of the accident, however, the policy was still in the process of being implemented.

Mental model flaws:

Skyguide management had delegated approval for Single Manned Operation Procedures (SMOP) to local operational management, and had published a set of regulations under which these procedures were allowed. This indicates that management felt that single manned operations were safe at least under certain conditions. Although SMOP was allowed during periods of low traffic, it was only to occur during the day, and night shifts were never approved for SMOP. During SMOP, a number of conditions had to be met including having additional controllers available in adjacent sectors and a supervisor to help the controller operating the single sector if needed. None of these conditions were met during the night shifts where only one controller was on duty. In addition, other conditions for SMOP included having the optical STCA be operational, having the
controller on a headset and having a fully functioning telephone system. On the night of
the collision, none of these conditions were met. The arrangement of having only one
controller on duty leaves no human redundancy to detect controller error, instead relying
on STCA to provide this redundancy. Despite prior incidents that had occurred during
SMOP, the practices had not changed, although additional features had been added to
ATC displays such as the range scale bar. These additional features were not available
on the night of the accident, and so there was no human or automation redundancy to
detect controller error.

**Inadequate control actions:**

Two controllers were responsible for controlling the entire airspace of ACC Zurich at
night according to the duty schedule. These two controllers had to assume the tasks of
the radar planning controller and the radar executive controller as well as the tasks of the
chief controller and the system manager. As a result, the continuous presence of a
controller at each workstation was not ensured during times such as prescribed breaks.
An addition, for years Skyguide management had tolerated the practice of allowing one
controller to take over the tasks of both controllers during periods of decreased traffic
flow while the second controller retired to the break room. This practice left one
controller on active duty, creating a situation where he would have to assume the tasks
normally filled by at least two people. Skyguide management did not do anything to
correct this unsafe practice.

Apparently, it was known that staff shortages work putting strain on controller workload
and forcing management to reduce service level; however, recruitment of additional staff
had fallen short of the required numbers, producing difficulties with rostering and
running training courses. For example, refresher courses were scheduled to be run every
six months, but were only carried out once per year. The staff shortages also had a
negative effect on staff moral with controllers perceiving them as a sign of lack of
support from management. Note, however, that according to Eurocontrol, there is a 12%
shortage of controllers throughout Europe.
In terms of training, controllers had not been sufficiently informed about operating the radar system in fallback mode. The controllers who worked the night shift were also expected to assume some of the duties of the supervisor, but were not trained to do so. Simulator training for emergency situations was also not available. Likewise, informational material regarding how to react to unusual situations was also not provided to controllers. Additional TRM (Team Resource Management) training was not available, but was not a requirement for Eurocontrol member states until November 2003. All in all, the training provided by Skyguide to its controllers was insufficient.

Coordination:

Skyguide’s Center of Competence (CoC), which was responsible for conducting risk-management activities, was not informed of the planned sectorization work. The cause for this might have been a lack of coordination that made it unclear whether it was the responsibility of Skyguide management or local ACC Zurich management to inform the CoC.

3.1.5 ACC Zurich

The analysis for this component in the system refers to the party responsible for issuing directives at ACC Zurich and approving maintenance work and controller practices. It is not clear exactly who is in charge of these functions, but for the purposes of this analysis that is not absolutely vital. What matters is the behavior and actions taken by this party.

Safety requirements and constraints:

Management at ACC Zurich was responsible for approving and coordinating scheduled maintenance work as well as overseeing practices in the control room. Issuing directives to keep the staff informed was also a task given to local management, as was the enforcement of safe practices. Management was also responsible for informing Skyguide’s Center of Competence and the adjacent air traffic control centers about planned maintenance work.
Mental model flaws:

Directives concerning the sectorization work had been issued and posted in the briefing room for controllers to read. Unfortunately there was no way to confirm that the controllers had actually read this information. Directives were also available at the supervisor’s console, but again there was no feedback mechanism to check whether the supervisor had briefed controllers about the directives.

ACC Zurich management may have also incorrectly assumed that based on SMOP during the day, that having only one controller during low traffic periods at night was sufficient. This assumption did not account for unusual situations such as decreased functionality of automation systems and unexpected aircraft like the delayed A320.

Inadequate control actions:

ACC Zurich management permitted a situation to occur where a single controller assisted by one assistant was responsible for controlling the entire low traffic flow of the center. The risks of this practice were not considered or documented. This caused an erosion of the system’s defenses, especially during a period of technical work.

Although SMOP (Single Manned Operation Procedures), whereby only one controller was on duty in a sector, was left to the discretion of local management to implement, it was never approved for night shifts where multiple day sectors were combined into one larger sector. Among other reasons, this was because at night there was no controller in an adjacent sector to help out if necessary, and no supervisor was available to supervise. ACC Zurich Management condoned the practice of having one of two assigned controllers retire to the break room while only one remained on duty.

Guidance was not provided to controllers regarding the handling of unusual situations. This guidance would have allowed a controller to evaluate the risks associated with a degraded technical system and adjust accordingly.

Although two written directives had been issued concerning the sectorization work (Z 2002-022 and Z 2002-024), these directives did not include a detailed description of the
consequences resulting from the system work in terms of the availability of technical equipment. As a result, even if the controllers had read the directives, they would not have been reminded of the capabilities of the radar system in fallback mode. Also, the controller on duty at the time of the accident was not made aware of the possible problem with the telephone system being down.

The controller on duty had not been informed that additional staff members were on duty to help him during the sectorization work. As a result, he assumed that he had to take over the tasks of the system manager as well during the night shift.

Also, a risk assessment concerning the affects of the sectorization work had not been carried out. No strategic planning had been done in advance to determine how to minimize the effects of the technical work, and the tactical management was left to the supervisor.

In the appendices of the BFU report, statements from other states in the investigation that deviate from those of the BFU are included. The Kingdom of Bahrain pointed out that management, knowing the consequences of the night’s maintenance work, should have briefed all staff involved about these consequences. The Kingdom of Bahrain went on to point out that management could have, at the very least, insisted that two controllers be on duty for that particular night given the layers of defense mechanisms that were missing due to the sectorization work. It is clear that management knew that the unsafe practice of having only one controller on duty would be made even less safe due to the temporary removal of automated warning aids such as optical STCA. Yet there were no attempts made to ensure that two controllers were available to make up for the loss of automation.

**Coordination:**

As mentioned above, Skyguide’s Center of Competence (CoC), which was responsible for conducting risk-management activities, was not informed of the planned sectorization work. The cause for this might have been a lack of coordination that made it unclear
whether it was the responsibility of Skyguide management or local ACC Zurich management to inform the CoC.

### 3.1.6 Skyguide Center of Competence (CoC)

#### Safety requirements and constraints:

Skyguide’s Center of Competence was responsible for the functions of safety, quality, audit and risk management within the company.

#### Context in which decisions made:

The CoC was experienced in the auditing and quality assurance functions when it was formed, but the safety and risk management functions had to be developed. Since the company decided to develop these capabilities in-house instead of bringing in outside expertise, the implementation of these aspects was delayed and they were still being implemented at the time of the accident.

#### Mental model flaws:

The CoC had not been informed about the sectorization work and therefore did not conduct a risk management study to minimize its impacts. Had the CoC known about the work, they might have been able to find workarounds to temporarily replace the systems that had to be switched off. They might have also recommended that both controllers remain on duty throughout the shift.

#### Inadequate control actions:

The quality assurance branch of Skyguide had known about the practice of allowing one controller to take over the tasks of both controllers during periods of decreased traffic flow, but no actions had ever been taken to correct the situation. This practice had been in place before the CoC was formed and was a result of past circumstances. In the past, three controllers were scheduled to work the night shift. One controller would retire to the break room while the remaining two controllers would work the shift. This practice was considered safe, as there were two controllers available to fulfill the night-shift tasks.
However, due to staff shortages a new practice began whereby only two controllers were assigned to the night shift. This new practice would have been safe enough if both controllers had remained on duty throughout the shifts; however, one controller continued to retire to the break room, leaving a single controller in charge of tasks designed to be performed by at least two controllers. The CoC did not correct this unsafe practice.

The CoC was not informed about the planned sectorization work and therefore did not undertake a risk assessment and mitigation process. This shows a lack of communication within the company and a breach of its own safety policy.

3.1.7 Supervisor who Briefed the Controllers at 21:00 hrs After his Shift

Safety requirements and constraints:

The supervisor’s briefing to the controllers at the shift change should have ensured that the controllers knew the operating environment, the temporary changes in effect, and the effects of those changes. Information on unusual conditions and an assessment of operational factors should have been included.

Coordination/Inadequate control actions:

The supervisor who finished his shift at 21:00 hrs did not include in his briefing any details of changes occurring because of the technical work because he considered that informing the controllers was the responsibility of the system manager. However, there were certain functions that were altered that related to the supervisor role. He did not focus on any operational issues resulting from the technical work, and he also did not indicate in any way that it might be wise to have two controllers working as a result of the lost automation features.

3.1.8 Departing System Manager

Safety requirements and constraints:

The system manager from the previous shift was responsible for briefing the controllers about any unusual occurrences in the operating environment that would affect their shift.
Coordination/Inadequate control actions:

The system manager did not brief the controllers on the implications of the sectorization work including the functions lost due to the radar system being in fallback mode. A lack of clearly defined roles led to the situation where it was unclear whose responsibility it was to brief the controllers.

3.1.9 Bulletin Board Containing Directives Regarding Technical Work

Safety requirements and constraints:

The bulletin board in the briefing room at ACC Zurich was used to post directives for controllers to read before their scheduled shifts. It was used as a means to convey pertinent information regarding the state of the system.

Inadequate control actions:

The directives regarding technical work that were posted on the bulletin board did not focus on the operational impact of the work. In addition, there was also no way to ensure that controllers read the information posted on the bulletin board. They did not read it. This illustrates a lack of feedback in the system, as there is no way for management to know if the controllers received the information or not.

3.1.10 ACAS/TCAS

While ACAS/TCAS is a completely automated system that functions independently of ATC, its implementation will be discussed here as part of the STAMP analysis of the accident because it is an integral part of the system.

Safety requirements and constraints:

ACAS/TCAS works independently of ground equipment, and functions independently of ATC as a last resort in preventing airborne collisions. Both the ATC system and the ACAS/TCAS system share the common task of collision avoidance. However, where
conflicts arise, an ACAS/TCAS RA takes priority, as defined by ICAO documents and the operations regulations of the aircraft operators. The TU154M’s flight operations manual, on the other hand, indicated that ATC had the highest priority in collision avoidance.

**Inadequate control actions:**

The implementation of ACAS/TCAS in the aircraft was deemed by the BFU report to be insufficient of its intended purpose, and did not correspond with ACAS/TCAS’ system philosophy. ACAS/TCAS regulations, procedures and operational instructions are published by ICAO, national aeronautical authorities, TCAS manufacturers and operators, and are not standardized among all these entities, leading to an incomplete and partially contradictory set of instructions on proper use. This confusion was cited by the BFU as a systemic causal factor leading to the accident.

Although there is an automatic downlink integrated into the TCAS system that sends RAs to the corresponding ATC units, at the time of the accident, it had not yet been implemented worldwide. The BFU recommended in their report that this downlink be installed.

### 3.1.11 Flight Operators

**Safety requirements and constraints:**

The flight operators were responsible for providing training programs to the flight crews on the operation of various systems in the aircraft including TCAS. They were also responsible for providing flight operations manuals that included instructions on the proper use of TCAS.

**Inadequate control actions:**

Both flight operators had provided training programs for TCAS to the respective flight crews. Practical TCAS training for the TU154M flight crew was not available as their simulator was not appropriately equipped. The flight operations manuals did not contain
detailed descriptions of the tasks of various crewmembers in case of a TCAS occurrence. The flight operations manual for the TU154M also indicated that ATC had the highest priority in collision avoidance. In certain scenarios, such as the one in this accident, following ATC instructions is a direct conflict with another statement in the manual that states that maneuvers contradictory to a TCAS RA are prohibited.

3.1.12 Controller at UAC Karlsruhe

Safety requirements and constraints:

The controller at UAC Karlsruhe was responsible for maintaining adequate separation between aircraft in his section of airspace, and responsible for coordinating with adjacent ATC centers. The controller at UAC Karlsruhe was alerted to the impending collision by his STCA. However, since the airspace was outside of his jurisdiction, he could only attempt to notify the controller ACC Zurich about the situation. His attempts were unsuccessful because a phone connection could not be established with ACC Zurich. Had he attempted to contact the aircraft directly by radio, he would have had to guess what frequency the aircraft were using, and if he had succeeded in contacting them, it is likely that this action would have just added to the confusion.

Mental model flaws:

The sectorization work at ACC Zurich had not been coordinated with adjacent ATC centers such as UAC Karlsruhe, who were not aware of any potential problems. Like the controller at ACC Zurich, they had not been informed that the direct telephone lines would not be available.

3.1.13 Controller at ACC Munich

Safety requirements and constraints:

The controller at ACC Munich was responsible for maintaining adequate separation between aircraft in his section of airspace, and responsible for coordinating with adjacent ATC centers. The controller at ACC Munich had just handed off the TU154M to ACC
Zurich, and confirmed the fact by noticing on his radar monitor that their transponder code had changed to 7520. He did not observe the impending collision as the aircraft had left his screen.

**Mental model flaws:**

The sectorization work at ACC Zurich had not been coordinated with adjacent ATC centers such as ACC Munich, who were not aware of any potential problems. Like the controller at ACC Zurich, they had not been informed that the direct telephone lines would not be available.

**3.1.14 System Manager and ATC Technical Expert Assisting Sectorization Work Technicians**

**Safety requirements and constraints:**

These two staff members were assigned to assist the technicians with sectorization work and had no responsibility to help the controller on active duty at ACC Zurich.

**Context in which decisions made:**

The system manager and the ATC technical expert assisting the sectorization work technicians were both qualified to recognize that the system degradations resulting from the work would negatively affect controller performance. They had no reason to believe, however, that appropriate risk-management measures had not been conducted, and that they should inform the controller of the degraded system conditions.

**Mental model flaws/Inadequate control actions:**

These staff members did not attempt to take any action to assist the controller in handling the effects of the sectorization work because they assumed that they were not responsible for doing so.
3.1.15 Technical Expert Assigned to Assist Controllers During the Sectorization Work

**Safety requirements and constraints:**

A technical expert was available to support controllers during the sectorization work if asked. His job was to ensure that the sectorization work did not interfere with normal operations.

**Mental model flaws/Inadequate control actions:**

The technical expert was not a controller and was not able to assess the working conditions of the controller in the current environment. As he was about to intervene, the controller had apparently already found a solution to the problem and so his help seemed to be no longer needed. The controller was not informed about this supporting expert and so did not ask for his help.

This technical expert and the other two support staff mentioned above did not recognize the increasing stress on the controller and so did not attempt to aid him in any way. They had not undergone human performance or TRM (Team Resource Management) training that would have allowed them to assess the situation.

3.1.16 Controller Assistant Aiding the Controller

At the beginning of the shift, there were two controller assistants assigned to aid the two controllers. Shortly after one controller retired to the break room to rest, one of the assistants also left. The remaining assistant had no authorization to assume any ATC functions. The controller at ACC Zurich did not delegate the task of communicating with Friedrichshafen to the controller assistant, as there was not enough time to do so.

**Safety requirements and constraints:**

The controller assistant’s job was to assist the controller with menial tasks such as printing flight strips. He was not authorized or trained to perform any ATC functions.
Inadequate control actions:

Although the controller assistant aiding the controller was aware of a third way to contact Friedrichshafen through the mobile phone at the supervisor’s workstation, he did not mention this fact as he felt that he might be stepping on the controller’s toes in doing so. This shows that perhaps a better relationship needs to be fostered between controllers and assistants. One way to do this might be to have controllers and assistants work in regular teams in the same manner as flight crews, who often spend several continuous flights working together.

3.1.17 SWI-02 & Bypass Telephone Systems

Safety requirements and constraints:

The SWI-02 and bypass telephone systems were used to communicate with adjacent ATC centers during both normal and emergency scenarios.

Inadequate control actions:

The SWI-02 telephone system that connected ACC Zurich directly to adjacent ATC centers such as UAC Karlsruhe and ACC Munich was not available as a result of the sectorization work. A failure in the bypass telephone system caused that system to be unavailable as well while the controller at ACC Zurich was trying to contact Friedrichshafen. By the time the bypass telephone system had been returned to service, the controller was already completely occupied with the A320, and did not answer three calls from the controller at UAC Karlsruhe who had been alerted to the conflict situation by the STCA there.

3.1.18 Optical STCA

Safety requirements and constraints:

The optical STCA (Short Term Conflict Alert) is designed to alert controllers of possible separation infringements, but does not automatically carry out any actions or make recommendations on how to correct the situation.
Inadequate control actions:

Had it been working, the optical STCA would have alerted the controller to the impending accident 2.5 minutes before the accident and the warning would have been available at both the radar planning and radar executive consoles. This would have given the controller plenty of time to correct the situation and prevented a TCAS advisory from even being issued. Note that STCA is considered to be an additional safety system, and ATC should function correctly even without it. However, the controller was not aware that the optical STCA had been turned off. Had he been briefed on this fact, he might have adapted his practices accordingly to be more conservative. Prior incidents had shown that in situations where only one controller was on duty, the lack of human redundancy to detect controller error was substituted by STCA warnings.

3.1.19 Aural STCA

Safety requirements and constraints:

The aural STCA was designed to sound once to alert the controller when the distance between two aircraft dropped below 6.5 NM.

Inadequate control actions:

No one in the control room recalled hearing the aural STCA. Had the controller heard the warning, it would have simply served to reinforce the urgency of the situation. Had the controller also recognized that the situation was not what he thought it was, it probably would have been too late by the time the warning sounded to correct it. In other words, the aural STCA is not very effective in cases of separation infringement occurring at high speeds.

In addition, the aural STCA does not keep sounding until it has been acknowledged. An improvement to the system would be to add confirmation that the controller received the alert by having the alarm continue until it was manually shut off by the controller.
3.1.20 Summary of Individual Component Analysis

In this section different components involved in the accident were analyzed to determine their roles in the system. A number of issues were identified and these in turn led to causes of the accident. These causes in turn lead to recommendations for how to improve the system.

The following issues were identified from the component analysis:

1. The unsafe practice of having only one controller on active duty during the night shift was known to, and tolerated by ACC Zurich, Skyguide management and Skyguide's CoC, which was responsible for maintaining safe practices.

2. Insufficient training was provided for staff. Controllers did not receive enough basic and refresher training, and also received inadequate training to deal with emergency situations. Supervisors did not receive sufficient training to identify potential problems that could arise due to maintenance work.

3. Directives issued by management about the sectorization work were unclear and incomplete. In addition, the methods used to disseminate the information were ineffective partially because the roles of the various parties involved in briefing the controllers were not clearly defined.

4. Controller assistants did not speak up about potential ways to help the controller since they were afraid of stepping on the toes of the controller.

5. Regulations and procedures regarding the proper use of ACAS/TCAS were unclear and sometimes contradictory, leading the crew of the TU154M to disobey the resolution advisory that they received.

6. ACAS/TCAS advisories were not available to air traffic controllers on the ground.

7. Skyguide management did not inform Skyguide's CoC about the scheduled sectorization work, and as a result, no risk management was conducted to minimize the impact of the work on normal operations.

8. The controller's dependence on the optical STCA in combination with his being occupied with dealing with the delayed A320 caused him not to notice the imminent separation infringement in time.

Comparing these issues with the ones found by the BFU, we notice that some of them link to the BFU’s immediate and systemic causes. The causes that the BFU found were listed earlier in section 2.2. Number 1 from above corresponds to BFU systematic cause number 2 and number 3. Number 5 corresponds to BFU systematic cause number 1 and immediate cause number 2, and number 8 corresponds to BFU immediate cause number 1. This serves as a good check of the STAMP analysis since the issues identified include those found in the official investigation report. In the section 5 of this thesis, the
recommendations drawn from the STAMP model will be compared to those made by the BFU in its accident investigation report.

The next section deals with how these components were linked together in the system centered on the controller at ACC Zurich, while the section after that on the system dynamics of the model tries to answer the question of how the problems found above came into existence.

3.2 Component Interactions

This section takes a look at how the components in the system were linked together. A block diagram first illustrates the theoretical control diagram that should have linked the components together. This is followed by a series of figures that show the degradation of the communication links due to various factors. Each succeeding figure is cumulative, meaning that the links removed in a preceding figure are also removed in later diagrams.

Figure 1 shows how the different components in the system should be connected by communications links in theory. Note that both physical connections such as phone lines as well as information flows such as procedures and reports are included in this diagram. Dashed links refer to partial connections, i.e. those that were not available 100% of the time. For example, only partial communications were available between the controller and multiple aircraft because only one party could transmit at a time when they were sharing a single radio frequency. Also note that the controller could not directly receive information about TCAS advisories, and that communicating all the time with all the aircraft actually required one controller at each of two consoles.
Figure 1: Components Surrounding the Controller at ACC Zurich

Figure 2: Links Degraded Due to Poor or Unsafe Practices
Figure 2 shows communications links that were broken or ineffective due to unsafe practices. These degraded links are shown in gray. They consisted of the inadequate briefings about the state of the system given by various parties to the two controllers scheduled to work the night shift, as well as the inability of the resting controller to aid the first controller in emergency situations due to the physical distance between the break room and the control room. The inadequate briefings were due to a lack of information as well as each party believing that they were not responsible for conveying particular information. The latter problem was a result of poorly defined roles. The feedback loop from the safety reports was broken here because management tolerated the unsafe practice of having only one controller on duty. Also removed are the controller assistant’s verbal comments to the controller. The controller assistant did not speak up with ideas to ease the situation because he felt that the controller might think that he was overstepping his bounds. The controller assistant’s perception of the relationship between controllers and controller assistants was the result of the attitude that some controllers had towards controller assistants.

Figure 3 removes the physical communications links that were missing due to the sectorization work. These include the direct SWI-02 phone system and the optical STCA warning. The removal of the primary SWI-02 phone system meant that the direct phone lines used to communicate with adjacent ATC centers were no longer available.
Figure 3: Links Lost Due to Sectorization Work

Figure 4: Links Lost Due to Unusual Situations
Figure 4 shows the effect of additional unusual situations such as the failure of the bypass telephone system and the appearance of the delayed A320. The appearance of the A320 meant that a separate console had to be used to control the approach sector for St. Gallen-Altenrhein and Friedrichshafen. As a result the controller had to alternate between the two consoles to communicate with all the aircraft, changing all the aircraft-controller links to partial ones.

Figure 5: Links Effectively Lost Due to the Controller Being Unaware of their Existence

Figure 5 shows the links there were unused because the controller did not realize that they were available. These include possible help from the other staff present in the control room and the third telephone system that the controller did not know about. This figure also removes the Aural STCA’s warning, which, although apparently functioning, was not heard by anyone in the control room. In addition, the link between the TU154M’s TCAS unit and the TU154M crew was effectively severed due to the crew ignoring the resolution advisory. At this point it is apparent that there were no complete feedback loops left in the system, and the remaining connections were mostly partial ones. The exception was the connection between the TCAS units of the two aircraft,
which were still communicating with each other. However, because the TCAS unit could only provide information to the crew, this remaining loop was unable to exert any control over the aircraft.

### 3.2.1 Communications breakdown on the night of the accident

From the set of figures above, it is obvious that one of the major factors contributing to the accident was the communications breakdown. The links were broken for various reasons. Some were the result of unsafe practices such as allowing only one controller to remain on duty during the night shift. Others, like the nonfunctional SWI-02 phone system, were caused by sectorization work, while more were the result of additional unusual occurrences such as the arrival of the delayed A320. Finally, some links were effectively removed even though they physically existed because the controller was unaware that they existed in the first place. This near-complete communications failure and the many different factors that contributed to it illustrate how different factors can combine to produce a major problem.
4 A System Dynamics Model of the Control Room Environment at ACC Zurich

STAMP is able to identify where safety requirements and constraints degrade slowly over time to result in an unsafe situation. Although a single behavioral adaptation may not have any negative effects when viewed alone, its evolution at a different pace than another variable may cause situations of degraded safety to develop. STAMP also allows the interactions of different variables to be visualized and analyzed to determine if those interactions lead to unsafe conditions.

In this section, a system dynamics analysis will be performed that focuses on the control room environment at ACC Zurich. Note that this analysis could also be performed on other important contributing factors to the accident such as the safety culture at Skyguide or the confusion and non-standardization of TCAS instructions and regulations across different authorities leading to the TU154M crew’s disregard of their TCAS RA to climb. In this example, the control room environment is relevant to determining the factors that affected the behaviors of the controller in charge of the aircraft and the other people who were present.

Figure 6 shows a system dynamics model for the control room environment at ACC Zurich. The model consists of several variables that affect each other in positive and negative ways. Variables that appear to be sources or sinks on the edge of the model interface with other parts of the larger system surrounding the control room. Each of the following sections will focus on a particular aspect of behavior taken from the larger model in Figure 6. The selected behaviors correspond to issues identified previously during the static analysis of components:

1. The practice of having only one controller on active duty during the night shift
2. Staff training
3. Unclear and incomplete directives
4. Controller assistants’ perception of controllers’ attitudes
5. Sectorization work and risk management to limit its impact
6. Dependencies that develop over time

The interactions of the variables within these groups determine how they evolve over time, and how they affect the most important variable in the system: Accident/incident Occurrences.
Figure 6: A System Dynamics Model of the Control Room Environment at ACC Zurich During the Night Shift.
4.1 The Practice of Having Only One Controller on Active Duty During the Night Shift

Figure 7 shows a portion of Figure 6 that illustrates why the practice of having only one controller on duty was tolerated by management.

The model demonstrates how a shortage of controllers coupled with a history of safe operations increased management tolerance of low staffing levels, thus increasing the risk of accidents, as shown by the balancing loop B1. When there are few incidents or accidents it is difficult for managers to maintain an emphasis on safety in the face of external pressures. In this case, managers tolerated a reduction from three to two controllers working the night shift. With only two controllers scheduled, there will only be one controller on active duty when the other controller takes breaks. One controller may not be able to manage all situations on his own. The risk of accidents therefore increases. The problem of declining safety consciousness is difficult to address. One way of addressing this particular problem would be for the government to impose regulatory requirements
regarding the minimum number of controllers on active duty during a shift. Such
requirements would force ATC companies to ensure that staffing is sufficient.
Furthermore, the source of pressure, the shortage of controllers, must be addressed.
Increasing recruitment efforts would be one way to address this source of pressure.

In addition, work habits that developed during, and were appropriate to, periods of high
staffing persisted when the staffing levels dropped. These habits further increased the risk
of accidents. Originally, three controllers were assigned to the night shift so that one could
rest while the other two worked. Over time the third controller’s break was extended
during periods of low traffic. When the lack of staff led to rostering only two controllers
for the night shift, one controller continued to take an extended break during periods of low
traffic. Longer breaks meant that controllers were left on their own for longer periods of
time, further increasing the risk of accidents. This situation was an example of
asynchronous evolution leading to unsafe practices. Thus, the root of the problem lay in
low recruitment and the evolution of a formerly safe practice into an unsafe one.
Supervisors and management should have informed controllers that extended breaks were
no longer permitted when there were only two controllers on duty. In addition, supervisors
should monitor controllers to ensure that they are no longer taking extended breaks.

4.2 Staff Training and Experience

Figure 8 displays the variables of the model related to training for air traffic controllers and
supervisors. The diagram shows that insufficient training both for controllers and
supervisors was a contributing factor towards increasing the Potential for Accidents. This
lack of sufficient training was partially due to there being not enough time for refresher
training for controllers. According to standard practices, refresher training was to be held
every six months; however, due to a staff shortage, this training was reduced to one session
per year. Staff experience was able to make up for some of this refresher training, but it
could not replace training for unusual occurrences. Sufficient practical training for
emergency procedures using simulators was not conducted, nor was training to educate
controllers about the degraded capabilities of the radar system in fallback mode.
The controller on duty did not receive any human factors training either when he initially trained to be an air traffic control officer in the early 1990s or through any additional training later. As a result, his team management skills stemmed from his personality and experience, and his knowledge of human error was also based on personal experience. The controllers who worked the night shift were also expected to assume some of the supervisor's duties; however, since the controllers were not trained as supervisors, they often attacked problems from the point of view of a controller instead of the point of view of a supervisor. Thus the controller on duty on the night of the accident lacked the ability to manage team resources and identify the situation where his attention was almost completely absorbed by one problem, namely trying to contact Friedrichshafen for the delayed A320.

![Diagram: Variables Associated with Insufficient Training](image)

**Figure 8: Variables Associated with Insufficient Training**
In addition, the lack of training for supervisors limited the ability of the supervisor, who briefed the controllers on the night of the accident, to recognize safety issues that might arise due to the sectorization work being conducted. Had he recognized the safety issues, he might have instructed both controllers to remain on duty throughout the shift or at least relayed the hazards onto the controllers. Unfortunately, these actions did not occur. Nevertheless, the supervisor was not the only party to issue incomplete instructions. The lack of clear instructions and directives will be discussed in the next section.

### 4.3 Unclear and Incomplete Directives

The dynamics in this excerpt from the model (Figure 9) show the results of unclear and incomplete directives being issued by a number of parties including local management and the supervisor who briefed the controllers at the end of his shift on the night of the accident. It also shows that one of the mediums used to disseminate information, namely the bulletin board used for directives from management, was ineffective. There were two major problems with the way information about the sectorization work was communicated. The first involved the mediums that were used. The directives regarding the sectorization work were posted on the bulletin board in the briefing room for controllers to read and also placed at the supervisor’s workstation. Neither of these methods was effective since the controllers did not read the information on the bulletin board and the supervisor’s briefing to the controllers was incomplete. The second problem was that the directives themselves were incomplete and did not give a detailed account of what the effects of the sectorization work would be. For example, they did not mention that the optical STCA warning system would not be available that night.
Figure 9: Variables Relating to Directives about the Planned Sectorization Work

It is easy to blame the controllers for not reading the directives regarding the sectorization work that were posted on the bulletin board in the briefing room. Looking deeper and contemplating the question of why they did not read the directives leads to the conclusion that perhaps the reason behind this behavior was that in the past the posted information was either incomplete or poorly written.

Another reason for complete information not being passed on to the controllers is that the different parties responsible for issuing the instructions, including the supervisor, did not
feel it was their job to do so. The supervisor felt that it was the system manager's job to brief the controllers on the details of the effects of the sectorization work. This confusion was the result of low Clarity of Role Definitions, meaning that whose job it was to inform the controllers about the details of the sectorization work was not clearly defined.

As a result of the lack of information, the Ability of Controllers to Estimate the Potential Risks Arising from Maintenance Work was compromised because they were unaware of how exactly the conditions in the control room would change. Also, better directives from management could have reminded the controllers which automated tools were available in the fallback radar mode, leading to increased Controller Awareness of Available Resources in Degraded Radar Modes. Had they been better informed with better directives, the controllers might have decided that they both needed to be present to make up for the decrease in automated warning systems and communications systems.

It is important to note that there is no independent feedback mechanism in place to determine whether the controllers received the proper information. Management's use of bulletin boards to disseminate vital information was flawed, as there was no method to check whether the information was received. One way to add this feedback to the system would have been for the supervisor to ask the controllers whether they had read the information on the bulletin board. Unfortunately, in the actual system the only way to know whether information was received was through interviews conducted during the accident investigation, by which time it was too late to prevent the accident from happening. Thus, this portion of the model shows how the unclear and incomplete directives issued by various parties contributed to the unsafe conditions present on the night of the accident.

4.4 Controller Assistants' Perception of Controllers' Attitudes

This section focuses on variables that were not discussed in much detail in the BFU's report. These variables concern the controller assistants' perception of the controllers' attitudes towards them, and Figure 10 shows how they affect Controller Workload and Controller Situational Awareness. Apparently one of the controller assistants (CAs) that
was scheduled to work on the night of the accident knew that there was a third mobile phone available at the supervisor’s console that could be used to contact Friedrichshafen; however, he did not bring up this information as he felt that in doing so he might be stepping on the toes of the controller. It might also have been possible for the controller assistant to ease the pressure on the controller by helping him with some of his tasks; however, in addition to the controller accepting the assistant’s aid, the assistant would also have had to notice that the controller was in need of help. As the controller assistant did not have the relevant human factors training, he did not notice the strain on the controller due to increased workload.

![Figure 10: Variables Related to Controller Assistants' Perception of Controllers' Attitudes Towards Them](image)

In order to create favorable conditions for controller assistants to offer their assistance, it might be a good idea to adopt the practice of scheduling crews of controllers and assistants to work together in regular teams in a similar manner to how airlines schedule flight crews to work together on multiple consecutive flights. It is not clear whether this practice is already in place or not, but it would build trust among the team and foster an environment where members would feel like they could contribute when necessary. It would also build the controller’s confidence in the team and therefore allow him to manage the team better, especially in unusual situations.

### 4.5 Sectorization Work and Risk Management to Limit its Impact

Figure 11 shows the affects of sectorization work and risk management to limit its impact. Referring to Figure 11, it is apparent that the Sectorization Work directly caused
Functionality of Communication System and Functionality of Radar System to be decreased. The first of these two effects meant that the controller needed to find other ways to communicate with Friedrichshafen and it also made it more difficult, if not impossible, for the controller at UAC Karlsruhe, who had noticed the impending collision, to contact the controller at ACC Zurich. The second effect meant that certain features of the radar system including the optical STCA warning were not available.

Assuming that a risk-management study had been conducted beforehand to minimize the impact of the sectorization work on normal operations, workarounds could have been created for the two effects mentioned above. Unfortunately, management failed to inform Skyguide’s Center of Competence, which was responsible for safety and risk-management, about the sectorization work, and ultimately no risk-management study was conducted. In addition, adjacent ATC centers such as UAC Karlsruhe had not been informed about the sectorization work and its effects, such as the disabling of the SWI-02 direct phone system. As a result, the disruption to normal routine caused by the sectorization work was much greater than it needed to be, further adding to unsafe conditions. Proper risk-management of the sectorization work could have minimized its effects on regular operations.
4.6 Dependencies that Develop Over Time

This subsection concerns habits that are difficult to break when the environment changes. The example here was the controller’s dependence on the optical STCA warning system. The optical STCA is meant to be an additional warning system, meaning that the air traffic control task should not rely on it. In other words, controllers should be able to maintain safe separation between aircraft without having the optical STCA. The problem with this philosophy is that when controllers use the optical STCA all the time for a long period of time, a dependency on it develops, even if the dependency is not supposed to exist by design. In other words, if a safeguard is available, people will use it because it makes their life easier, even if they are told not to depend on it, as it will not always be available. Combining this dependency with the fact that there was no explicit indication from the workstation that the optical STCA was not available produced the unsafe condition where the controller thought that the optical STCA was not reporting any conflicts because there were no separation infringements. Had the optical STCA been working, it would have alerted the controller to the impending separation infringement, causing him to separate the aircraft sooner. In this scenario, no TCAS advisories would have even been generated. Were the controller not dependent on the optical STCA, he would have used other means to determine whether the separation was in danger of being violated as part of his usual routine. Unfortunately, the controller’s dependency on the optical STCA warning combined with the fact that he did not realize it was not working produced a false trust in the automation to solve the problem, which it did not. This example illustrates that even though air traffic control is supposed to function without additional warning systems present, dependencies may develop over time that make the warning systems an integral part of the system.

4.7 Conclusion to Analysis Using the System Dynamics Model

A system dynamics model is a useful tool to visualize how the different variables in the system affect each other and combine to cause unsafe situations that can potentially lead to accidents. By looking at relevant parts of the model, conclusions can be drawn as to
the causes of both seemingly safe and irrational behaviors of the operators in the system. This section presented a system dynamics model of the control room environment at ACC Zurich on the night of the accident, and used it to answer questions such as why management tolerated having an insufficient number of controllers on duty during the night shift, and why unclear and incomplete directives were issued. The model also showed how interactions could change over time to produce unsafe conditions, such as the example of the controller’s dependency on the optical STCA warning system. As a result, additional insight was discovered on the issues found by the earlier component analysis. In the final section of this thesis, this additional insight will be used to generate recommendations that will be compared with the recommendations produced by the BFU.
5 Summary and Recommendations

The static analysis from the STAMP model of the Überlingen Aircraft Accident uncovered a number of systemic issues that led to the accident. The system dynamics model explored these issues further to determine how they arose. The issues found by the model were:

1. The unsafe practice of having only one controller on active duty during the night shift was known to, and tolerated by ACC Zurich, Skyguide management and Skyguide's CoC, which was responsible for maintaining safe practices.
2. Insufficient training was provided for staff. Controllers did not receive enough basic and refresher training, and also received inadequate training to deal with emergency situations. Supervisors did not receive sufficient training to identify potential problems that could arise due to maintenance work.
3. Directives issued by management about the sectorization work were unclear and incomplete. In addition, the methods used to disseminate the information were ineffective partially because the roles of the various parties involved in briefing the controllers were not clearly defined.
4. Controller assistants did not speak up about potential ways to help the controller since they were afraid of stepping on the toes of the controller.
5. Regulations and procedures regarding the proper use of ACAS/TCAS were unclear and sometimes contradictory, leading the crew of the TU154M to disobey the resolution advisory that they received.
6. ACAS/TCAS advisories were not available to air traffic controllers on the ground.
7. Skyguide management did not inform Skyguide's CoC about the scheduled sectorization work, and as a result, no risk management was conducted to minimize the impact of the work on normal operations.
8. The controller's dependence on the optical STCA in combination with his being occupied with dealing with the delayed A320 caused him not to notice the imminent separation infringement in time.

Recommendations can be obtained by looking how these issues arose.

5.1 The Practice of Having Only One Controller on Active Duty During the Night Shift

The system dynamics analysis concluded that this practice evolved from the practice of one controller taking extended breaks when there were three controllers scheduled to work the night shift. This developed into the unsafe practice of only one controller being
on duty when staff shortages reduced the number of scheduled controllers to two. The following recommendations are intended to address this problem:

1. Create and enforce regulations that stipulate that there must be at least two controllers on active duty at all times in each sector. This could mean that more than two controllers are scheduled so that breaks can be taken. The responsibility to enforce the regulations would be assigned to the Swiss Federal Office for Civil Aviation (FOCA), which would ensure that Skyguide management, supervisors and the controllers obeyed them. FOCA should periodically check the regulations created above to make sure that they are obeyed. When they are not obeyed, an effort must be made to find out why.

2. Attempt to reduce the shortage of controllers by increasing active recruitment of controllers.

The first recommendation corresponds to BFU Safety Recommendation No. 02/2003.

5.2 Insufficient Training and Refresher Training for Emergency Situations, Automation, Team Resource Management and Human Factors

The lack of sufficient training was a major factor that affected a number of variables including the controller’s ability to manage unusual situations, and the ability of other staff to recognize the strain of the degraded system on the controller. The following recommendations are intended to address this problem:

1. Conduct practical training for controllers that includes training for emergency procedures and what to expect when operating with a system of decreased functionality, e.g. during maintenance work.

2. Make sure that this training is repeated on a prescribed six-month schedule to refresh controllers’ memories and prevent them from forgetting the features available in degraded radar modes and becoming too dependent on automation.

These recommendations relating to training correspond to BFU Safety Recommendations Nos. 03/2003 and 21/2004.

5.3 Unclear and Incomplete Directives

The lack of clear and complete directives was a major cause of the communications breakdown that occurred on the night of the accident. Directives given by ACC Zurich to the controllers did not include details on the operational impact of the sectorization work. In addition, the method for transmitting the information via the bulletin board was ineffective because the controllers did not read the information on it. As a result, the
controllers and other staff were not able to prepare properly for the unusual conditions that occurred because of the maintenance work. In addition, the information about the impact of the sectorization work was not relayed via the supervisor’s briefing because he did not feel that it was his job to do so. A lack of clear definition of whose job it was to brief the controllers on the control room conditions caused the breakdown of information flow to occur. The following recommendations stem from this issue:

1. In directives regarding maintenance work, include the impact of the work on regular operations. Include reminders as to which automation tools are available and which are not. Also include information as to whether there are extra staff members on hand to provide assistance. The controller at ACC Zurich was unaware that a technical expert had been assigned to support the controllers, and hence did not know that he could ask the expert for help.

2. During planning for maintenance work, indicate clearly whose job it is to pass on information to various parties, and make sure that there are feedback mechanisms to ensure that the information has reached the intended parties.

3. Make sure that risk-management studies are carried out beforehand to minimize the impact of the maintenance work, and to inform controllers about the temporary changes.

These recommendations regarding directives correspond to points in BFU Safety Recommendations Nos. 01/2003 and 10/2004.

5.4 Controller Assistants’ Perception of Controllers’ Attitudes

Controller assistants hesitated to contribute ideas to help solve problems as they felt that they might be stepping on the toes of the controllers. In order to foster a relationship among controllers and assistants where assistants are not afraid to contribute, the following recommendation comes to mind:

1. Schedule teams of controllers and assistants to regularly work together so that trust can be built and the team can learn to function as a unit. This also improves the controller’s ability to manage the team in emergency situations.

This recommendation is not found in the BFU’s report.

5.5 ACAS/TCAS Regulations and Operational Procedures, and Flight Crew Training

The TU154M crew did not take into account that a TCAS RA involves two complementary instructions. The TU154M crew should have questioned the controller’s
instruction to descend since it was in direct opposition to the TCAS RA. This indicates that the crew did not know enough about how the TCAS system worked or at least momentarily forgot. ACAS/TCAS documentation is widely available, but the information is typically only available to pilots through company manuals in condensed form. In addition, regulations and operational procedures are published by a number of organizations including ICAO, Eurocontrol, flight operators and TCAS manufacturers. These regulations are confusing and often contradictory. Thus the following recommendations arise:

1. Require TCAS simulator training for crews flying TCAS-equipped aircraft.
2. Standardize TCAS regulations and procedures, and create a regulation that indicates that TCAS RAs take precedence over ATC instructions.
3. Implement the TCAS downlink to inform controllers about TCAS advisories.
4. Create regulations to require confirmation of instructions when TCAS and a controller contradict each other.

These recommendations correspond to BFU Safety Recommendations Nos. 18/2002, 06/2004, 07/2004, 08/2004, 15/2004, 16/2004, and 21/2004. Since the model in this thesis did not focus on TCAS, the recommendations found by the model were not as detailed as those from the BFU’s report.

5.6 Sectorization Work and Risk Management to Limit its Impact

The sectorization work was a major factor in creating unusual conditions in the control room that made it difficult for the controller to deal with the task of air traffic control. The loss of the SWI-02 phone system and automation systems not only decreased the tools available to the controller, but also increased his workload because he had to figure out another way to contact Friedrichshafen. He was also unaware that the optical STCA was not working, as he did not remember that it was not available in the fallback radar mode. There was no briefing to inform him of that fact either. Had a risk-management study been conducted, measures could have been taken to minimize the impact of the sectorization work on regular operations. A risk-management study had not been conducted, however, because management failed to inform the CoC about the sectorization work. According to Skyguide’s own safety policy, management should have involved Skyguide’s CoC in the planned sectorization work so that it could conduct
a risk assessment and produce risk mitigation strategies. In spite of this, the CoC was not informed of the technical work, and so could not complete an assessment of its impact on operations. In addition, adjacent ATC centers were not informed about the sectorization work or its effects such as the disconnection of the SWI-02 direct phone system. The following are recommendations related to the sectorization work and risk-management to limit its impact:

1. Require management to inform the CoC about all scheduled maintenance work.
2. Require risk-management studies to be completed before maintenance work is allowed to take place. These studies should not only determine the impact of the work, but also strive to minimize the number of systems that are affected.
3. Make sure that maintenance work is scheduled at times that minimize the impact on regular ATC operations.
4. Inform all relevant parties about the scheduled maintenance work, including controllers and adjacent ATC centers.

These recommendations correspond to BFU Safety Recommendation No. 17/2004.

5.7 Dependencies on Automation that Develop Over Time

The controller’s dependency on the optical STCA that developed over time caused him not to realize that the reason there were no warnings was because it was not available, and not because there were no conflicts. There were no indications on the radar screen regarding the unavailability of the optical STCA. Also, no directives had been issued concerning the lack of optical STCA either. The controller also did not remember that the optical STCA was not available in the fallback radar mode. This dependency on the automation created a situation where the controller was not doing his proper task of maintaining separation between aircraft, and there was no automated warning system to catch what he missed. Although it is easy to say that the controller should not have relied on the optical STCA, it would probably be more effective to make the following recommendations:

1. Add an indicator to the controller’s workstation to indicate when STCA or other automation systems are not available.
2. Provide refresher training on what tools are not available in degraded radar modes.
3. Provide briefings prior to maintenance work to inform controllers of the tools available during that shift.
The first recommendation corresponds to a point in BFU Safety Recommendation No. 10/2004. The second corresponds to BFU Safety Recommendation No. 19/2004 on refresher training.

5.8 Other Recommendations

In addition, a number of other recommendations stem from parts of the model that were not analyzed in detail. These include the redesign of some of the automation tools. For example, the aural STCA could be changed so that instead of sounding only once and then stopping, it would continue to sound until the controller acknowledged it. This would ensure that the controller noticed the warning. Another example involving automation design could be to add an additional warning system to the cockpit that would be activated when there was only one pilot in the cockpit in order to provide an extra line of defense against separation infringements. Another recommendation would be to increase the update frequency of the radar display. This recommendation stems from the fact that at the time that the controller issued the instruction to the TU154M to descend, the radar display had not updated to show that the B757-200 had already started to descend. The aural STCA is addressed in BFU Safety Recommendation No. 10/2004, while the radar system update frequency is addressed in BFU Safety Recommendation No. 12/2004.

Recommendations were developed in this section based on the analysis of the STAMP model. Many of the recommendations corresponded to recommendations that the BFU made in their official accident investigation report. The BFU had more detailed recommendations relating to TCAS than those presented in this thesis; however, this was expected since the STAMP model in this thesis did not focus on TCAS, but on the control room environment surrounding the air traffic controller on duty at the time of the accident. In regards to the control room environment, the STAMP analysis generated recommendations to match those of the official report, and also additional ones such as the development of staff teams that were scheduled to work together over multiple shifts in order to foster better team relationships and trust.
5.9 Conclusion

The system dynamics portion of STAMP allows the interactions over time of different variables in the system to be visualized. This in turn allows the question of why certain behaviors were observed in the system to be answered. It also shows how combinations of variables can work together to generate unsafe conditions even when no unsafe conditions can be detected from analyzing the individual components. Studying the issues raised by the model produces recommendations on how to solve the issues to prevent accidents from occurring in the future. The STAMP model was able to make recommendations that corresponded to the ones from the official accident investigation report and also additional recommendations that the BFU report did not include. These recommendations show that STAMP is an effective tool for analyzing aircraft accidents, as it is able to facilitate ease of analysis by allowing component interactions to be visualized. Further work could include extending the STAMP model to other aspects of the accident for a more complete analysis.
References


