

LINATE AND ÜBERLINGEN: UNDERSTANDING THE ROLE THAT PUBLIC POLICY PLAYS IN THE FAILURE OF AIR TRAFFIC MANAGEMENT SYSTEMS

Christopher W. Johnson

Glasgow Accident Analysis Group¹

Keywords: Air Traffic Management; Computer Systems; Accident Analysis.

Abstract

The terrorist attacks of September 2001 had significant economic effects on the aviation industries. Passenger numbers fell across many countries and several large carriers were threatened with bankruptcy. More recently, there has been a gradual recovery. This has renewed concern that the rising volume of traffic will lead to an increase in the total number of safety-related incidents as accident rates have remained stable. This creates a “wicked problem”. How can we further reduce the rate of very rare events before there is any rise in the total number of the accidents and incidents? There are no panaceas but it seems clear that we must identify any common factors that occur between the relatively small numbers of adverse events that occur each year. This paper, therefore, shows how violations and vulnerability (V2) analysis can be applied to identify similar causes in the Linate runway incursion and the Überlingen mid-air collision. Both stemmed from underlying problems in the Safety Management Systems that are designed to protect the European Air Traffic Management (ATM) infrastructure.

Introduction

From 1995 to 2000, the worldwide accident rate was 1 in every 1.25 million flights. This improved between 2001 and 2005 to 1 accident in every 2 million flights. In 2004, the European Air Traffic Control agency, EUROCONTROL, recorded a single mid-air collision that was directly caused by Air Traffic Management (ATM) involvement. This was not fatal. Such statistics illustrate the significant progress that pilots, Air Traffic Control Officers (ATCOs), managers and regulators have made in raising safety standards. However, passenger numbers are gradually increasing across many routes in the aftermath of the 2001 terrorist attacks. These increases in departures must be offset against further falls in the accident rate if we are to maintain or reduce the total annual number of annual incidents.

It is unclear how to achieve further safety improvements when the accident rate is already so low. These problems are compounded by the pathological combinations of events that seem to trigger adverse events in European air space. Many authors use Reason’s ‘Swiss Cheese’ model to characterize the bizarre way in which underlying vulnerabilities line-up in the events leading to major failures [7]. In contrast, the following pages argue that many accidents in European air space have a core set of common causes. In particular, violations and vulnerability (V2) analysis is used to identify the latent and catalytic events leading to the Linate runway incursion and the Überlingen mid-air collision.

¹ Glasgow Accident Analysis Group, Department of Computing Science, University of Glasgow, Glasgow, G12 8QQ, Scotland, U.K. johnson@dcs.gla.ac.uk, <http://www.dcs.gla.ac.uk/~johnson>

Overview of the Überlingen Accident

The Überlingen accident occurred on the 1st July 2002 when a Boeing 767-200 was involved in a mid-air collision with a Tupolov TU164M [2]. A total of 71 crew and passengers were killed on both aircraft. The immediate causes of the accident centered on the Air Traffic Control Officer's (ATCO) instruction to the Tupolov crew, which contradicted the Traffic Alert/Collision Avoidance System (TCAS) on-board warning system, and ordered them to descend into the Boeing 767 which was also responding to a TCAS warning to avoid the other aircraft. The official BFU report into the accident was issued in 2004. It provides a relatively thorough analysis of the causes that led to the confusion over the warning from the TCAS software. In contrast, this paper focuses on the infrastructure changes at the Zurich Air Traffic Control Center. Scheduled maintenance procedures created some of the preconditions where the ATCO was likely to make a mistake.

Overview of the Linate Accident

The Linate accident happened on the 8th October 2001 when a Boeing MD-87 was taking off from runway 36R at Milan's Linate Airport [1]. The MD-87 collided with a Cessna 525-A, which taxied onto the runway. The MD-87 carried two pilots, four attendants and one hundred and four passengers. The Cessna carried two pilots and two passengers. All occupants of the aircraft were killed along with four ground staff who were working in a baggage handling building struck by the MD-87 after the runway collision. The official ANSV report identified the human factors causes that led the Cessna's crew to mistakenly cross the active runway under, low visibility conditions. It also balanced these factors against a number of organizational and technical limitations in the systems in the airport's operational environment that created the preconditions for the accident.

Motivation

These accidents had a profound impact on both the Italian and Swiss Air Traffic Service Providers. They also motivated the European Strategic Safety Action Plan as national bodies moved to learn the lessons of the Überlingen and Linate accidents [6]. Most of these initiatives treated the incidents as separate events. For instance, reports into the Überlingen accident focused on the role of TCAS and on the management of the Zurich Center. Conversely, work on the Linate accident tended to focus on the problems of runway incursion. This is illustrated by the establishment of the European Action Plan for the Prevention of Runway Incursions [3]. None of these reports looked at the common element in both accidents. To date, there has not been any sustained consideration of similarities in the project management problems that affected the software infrastructure in the Linate and Überlingen accidents. The following pages, therefore, identify common causes between these adverse events.

Public Policy Tensions between Safety Regulation and Market Economics

Public policy is defined to be guidelines or rules that results from the actions of governmental and quasi-governmental organizations. Public concern over infrastructure reliability often persuades government agencies to intervene directly in the engineering of many large scale computer systems. There is considerable controversy over whether such interventions directly contribute to incidents and accidents. It can be argued that governmental intervention is necessary to ensure 'social goods', including reliability, that cannot be guaranteed under free market competition. In contrast, it is also argued that government intervention creates the preconditions for failures when deregulation fails to consider the implications for infrastructure investment [4].

Both the Überlingen and Linate accidents have causes that stretch back into the public policy of Air Traffic Management in Italy and Switzerland. In both cases, national governments were struggling to resolve the tensions between market economics and the need to maintain extremely high levels of safety. For example, the Swiss government began to reduce direct

State intervention in ATM service provision during the 1980s and early 1990s. Swisscontrol became an independent joint stock company under Swiss law in 1996. A key objective in this process was for airlines and airports to meet the financial costs associated with air navigation service provision rather than Swiss tax payers. Skyguide was formed in 2001, by the merger of military and civil air traffic management. Figure 1 sketches the management and regulatory structures surrounding this company in the months prior to the Überlingen accident [8]. The Swiss Confederation retained formal owner of Skyguide with a majority shareholding. As can be seen, the Federal government was represented by the Department of Defense, Protection and Sport (DDPS) and the Department of Environment, Transport, Energy and Communication (DETEC). DDPS focused on the need to integrate civil and military service provision. In contrast, DETEC was primarily concerned to ensure that Skyguide operated at no cost to the Swiss Confederation. This created important tensions given the rising volume of air traffic and the international agreements that place caps on the levies raised against air traffic. These constraints were exacerbated by the obligations to maintain services in areas that would normally not have been financially viable, including smaller airfields. Skyguide were placed under further financial pressures in the years leading to the accident by accounting structures that made it difficult for them to carry forward financial reserves as a contingency against future difficulties.

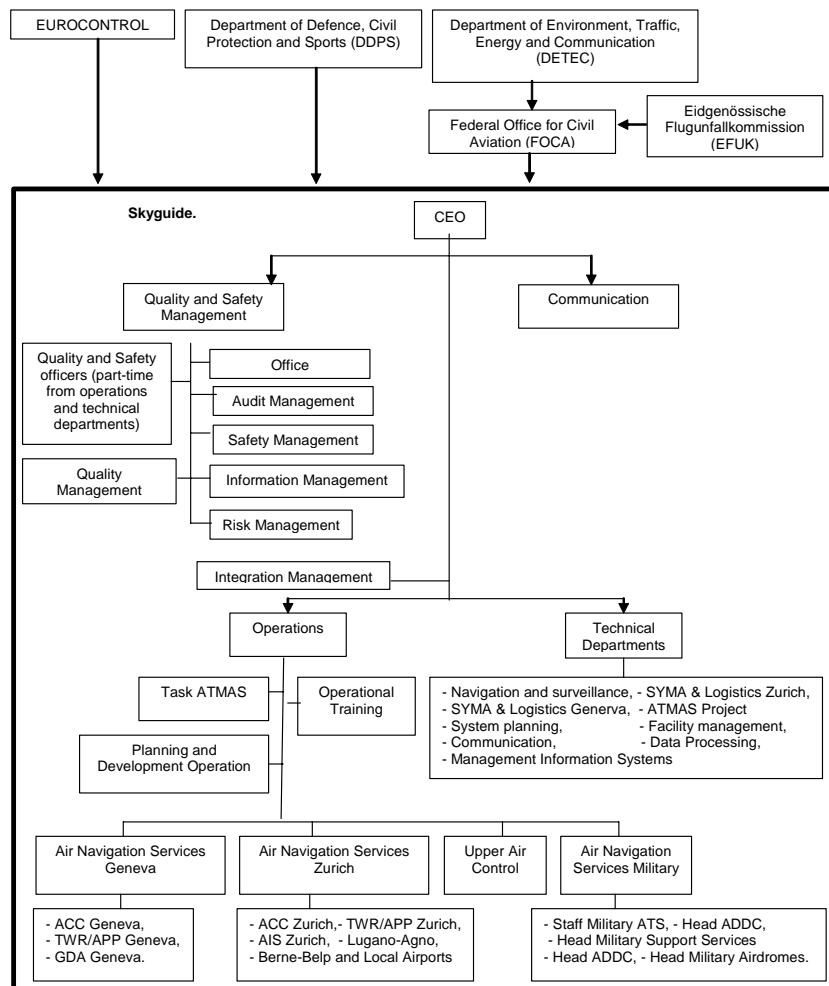


Figure 1: Simplified Skyguide Organisational Structure Prior to the Überlingen Accident

Figure 1 can be used to identify further tensions in the public policy towards Air Traffic Service provision leading to the Überlingen accident. Aviation was one of many different concerns for the Department of Environment, Transport, Energy and Communication

(DETEC). They also lacked specific expertise in aviation safety. In practice, responsibility for aviation was largely devolved to the Federal Office for Civil Aviation. However, the interface between these organizations relied on personal meetings between the director of FOCA and the minister. Figure 1 also illustrates the dual nature of the Federal relationship with Skyguide. On the one hand DETEC and FOCA had a regulatory role in ensuring the safety of service provision. On the other hand, DETEC and DDPS were representatives of the majority (state) shareholders in Skyguide. In public policy terms, this led to the development of an elaborate supervisory system (ASN Aufsichtskonzept). A subsequent government sponsored report found that “...with regard to Skyguide, safety is an aspect of both the regulatory relation and the ownership relation with the government. This could lead to a situation where the accountability for safety is not clear” [8].

Public policy created a tension between safety requirements and neutral-cost service provision in Skyguide. Figure 2 shows how the operational staff at Linate were also caught between the economic competition and safety regulation. These are represented by the Ministero delle Infrastrutture e dei Trasporti and the Ministero dell’Economia e delle Finanze. This is a common tension in modern air traffic management as market forces play an increasing role in former state monopolies. Perceived changes in the priorities associated with economic competitiveness and with safety regulation have also been identified as root causes of accidents in a wide range of industries, as diverse as UK railways and US space missions [5].

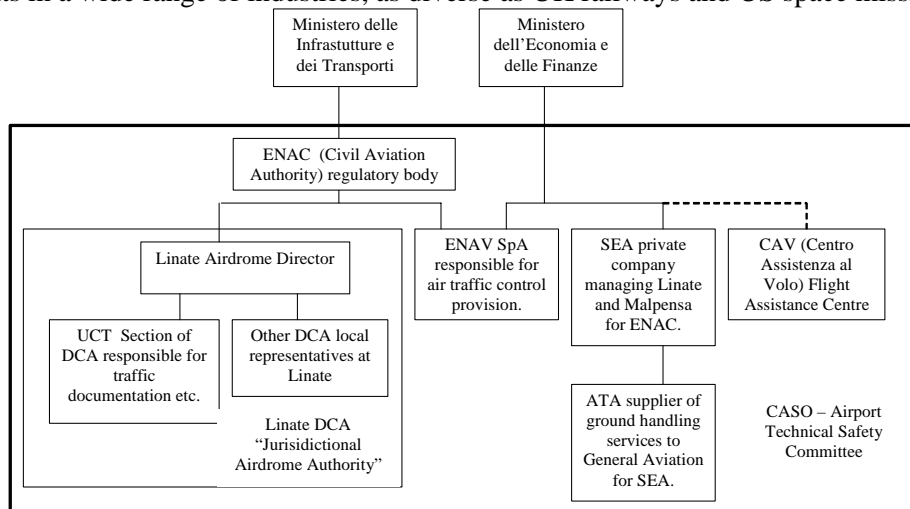


Figure 2: Simplified Organisational Structure Prior to the Linate Accident

The public policy tensions between infrastructure provision and economic competitiveness led to a complex division of responsibilities at Linate. The service provider, ENAV, was controlled by the ministry of finance but operated under ‘surveillance’ from the ministry of transport. The official investigation concluded that “the management and operational situation at the airport was complicated and involved three major organizations ENAC (Italian Civil Aviation Authority), ENAV (Air Navigation Service Provider) and SEA (company managing Linate airport for ENAC). No effective performance agreements did exist between involved organizations regarding safety matters” [1].

Figures 1 and 2 set the scene for both accidents. The divided reporting structures for Skyguide made it difficult to implement effective safety management systems. Under financial pressure, the company sought to develop these systems themselves rather than incur the overheads associated with outside expertise. This decision resulted in inevitable delays and partly explains the lack of adequate risk mitigation in the events leading to the Überlingen accident. At Linate, the multi-party reporting and management structure led to many organizational difficulties. In particular, the ANSV argued that the divided reporting

illustrated in Figure 2 prevented the airport authorities from fully developing appropriate Safety Management Systems.

The Impact of Public Policy on Safety Management Systems

The organisational and regulatory structures in Figures 1 and 2 illustrate the context in which the Linate and Überlingen accidents occurred. However, these diagrams offer little benefit unless they provide more detailed insights into the events that led to these ATM-related failures. One means of doing this is through the use of Violation and Vulnerability (V2) diagrams. Figure 3 applies this technique to represent more immediate causes of the Überlingen accident. The analysis of public policy effects on organizational structures in Figure 1 reinforced the conclusion from the original reports that "...with regard to Skyguide, safety is an aspect of both the regulatory relation and the ownership relation with the government. This could lead to a situation where the accountability for safety is not clear". Figure 3 introduces this as a vulnerability denoted by a double ellipse that can be associated with problems both in the safety management and safety culture of the organizations concerned. These consequent vulnerabilities are linked to observations on page 91 of the BFU report [2].

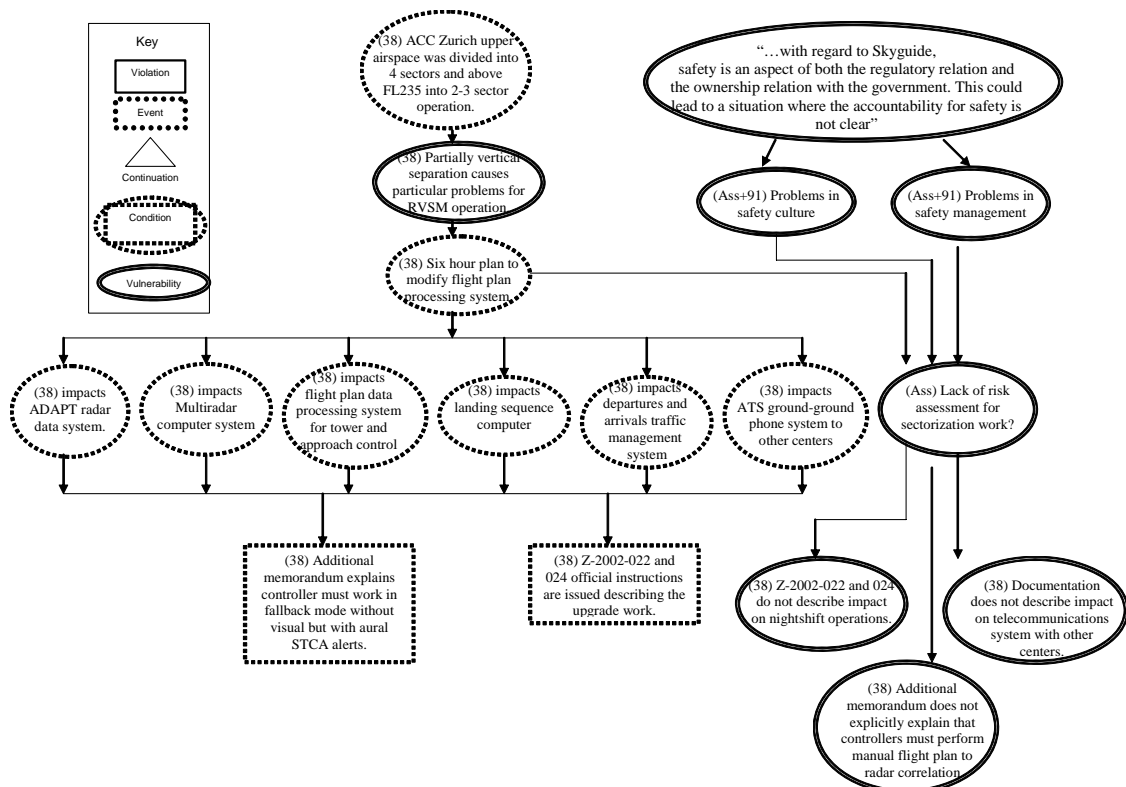


Figure 3: Public Policy Influences on the Technical Infrastructure in Zurich ACC

The V2 diagram in Figure 3 also illustrates how a plan to upgrade the technical infrastructure in one of Skyguide's control centers exposed the vulnerabilities, created by particular public policy decisions. ACC Zurich upper airspace was divided both vertically and horizontally. The particular vertical division about FL235 into 2 or 3 sector operations created particular problems for the operation of Revised Vertical Separation Minima (RVSM). RVSM was a European initiative to increase capacity by relying on new generations of avionics to reduce the vertical separation between aircraft. ACC Zurich staff, therefore, developed a six hour plan to modify the flight plan processing system to simplify the upper airspace and support the implementation of RVSM. This plan effected a number of different systems: the ADAPT radar data application; the multi-radar computer system; the flight plan data processing system for tower and approach control; the landing sequence computer; the departures and

arrivals traffic system and the ATS ground to ground phone system with neighboring centers. A further consequence of these effects was that management began to prepare for the upgrade by issuing official instructions Z-2002-022 and 024 to describe the work. An additional memorandum also documented the impact that the work would have in requiring controllers to work in fallback mode without a visual STCA. The key point here is that V2 diagrams provided a means of tracing the interaction between public policy, safety management and the detailed technical infrastructure supporting ANSP staff during the Überlingen accident.

As mentioned, the ANSV report concluded that “the management and operational situation at the (Linate) airport was complicated and involved three major organizations ENAC (Italian Civil Aviation Authority), ENAV (Air Navigation Service Provider) and SEA (company managing Linate airport for ENAC). No effective performance agreements did exist between involved organizations regarding safety matters” [1]. The official report goes on to link this structure to the lack of an effective Safety Management System, see page 116 [1]. Figure 4 relates this vulnerability to deficiencies in the ground operations just as Figure 3 sketched the relationship between public policy and safety management for the Überlingen accident.

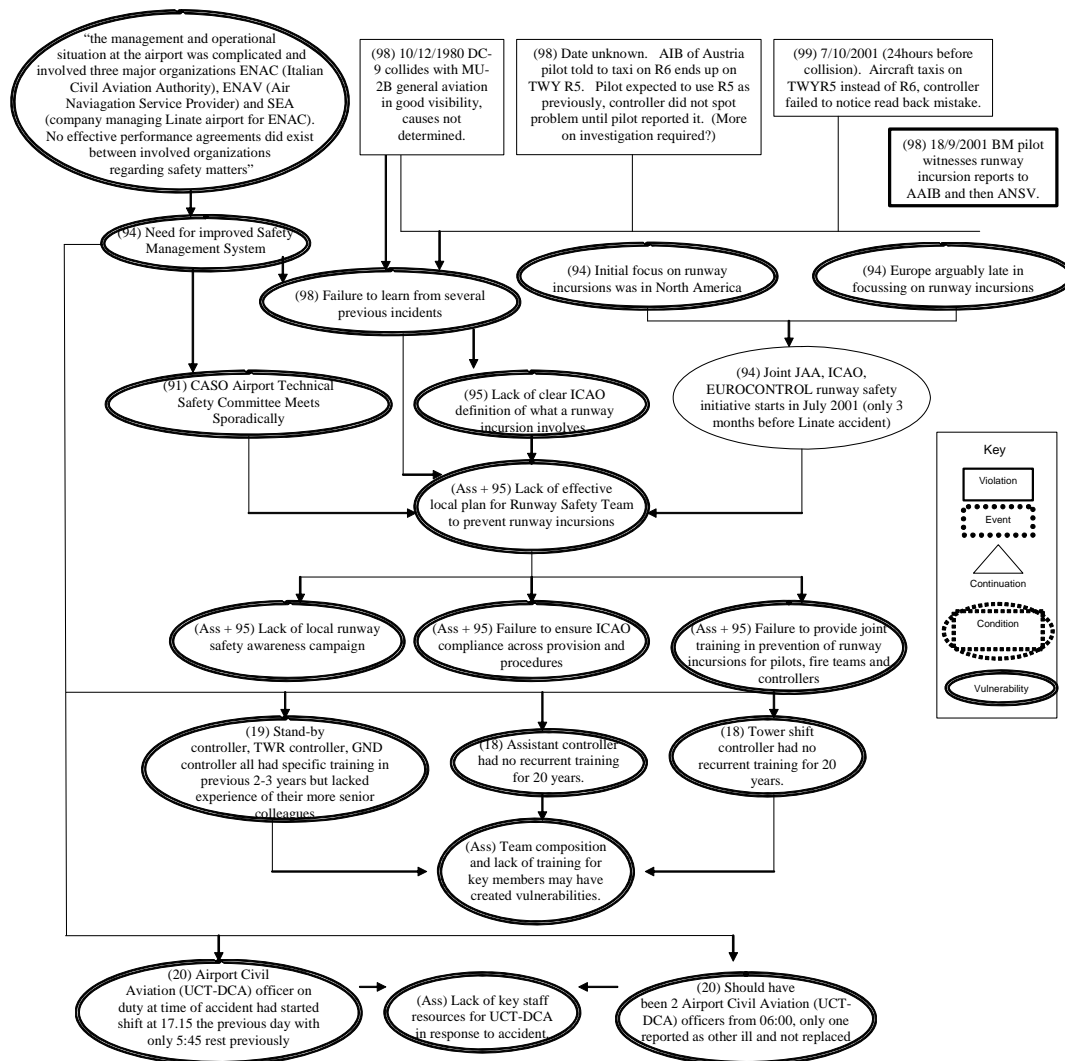


Figure 4: Public Policy Influences on the Organisational Infrastructure at Linate Airport

The problems in safety management at Linate also help to explain a failure to learn from previous incidents. These are shown in Figure 4 as four separate events, including a very similar incident to the collision between the Cessna and the MD-87 which occurred only 24

hours before the accident. The V2 diagram also links the lack of an effective runway safety plan to problems in safety management which can, in turn, be linked back to public policy issues.

High Tolerance for Reduced Staffing Levels

Too is often an undue focus on the technical infrastructure in accidents and incidents. It is important not to overlook the critical role that human resources play both in the causes of, and response to, adverse events. For instance, Figure 3 links the need to improve Safety Management Systems to a lack of DCA (Airdrome Judicial Authority) and UCT (Traffic documentation section) staff. There would usually have been two UCT officers on duty at Linate but only one had turned up for duty. Fortunately, their colleague on the previous shift was still present even though they had worked a continuous total of 13 hours on duty. This had important consequences as Air Traffic Managers and emergency personnel responded to the collision. For now it is sufficient to observe that page 60 of the ANSV report lists a number of specific “failures to adhere to prescribed obligations”, including staffing levels. The key point is to identify specific ways in which high-level observations about the operation of Safety Management Systems led to specific vulnerabilities that were exposed during the accident. In this case, the lack of UCT staff and the problems in the shift patterns of those who were on duty, arguably, did little to exacerbate the consequences of the incident. In future accidents, we may not be so fortunate.

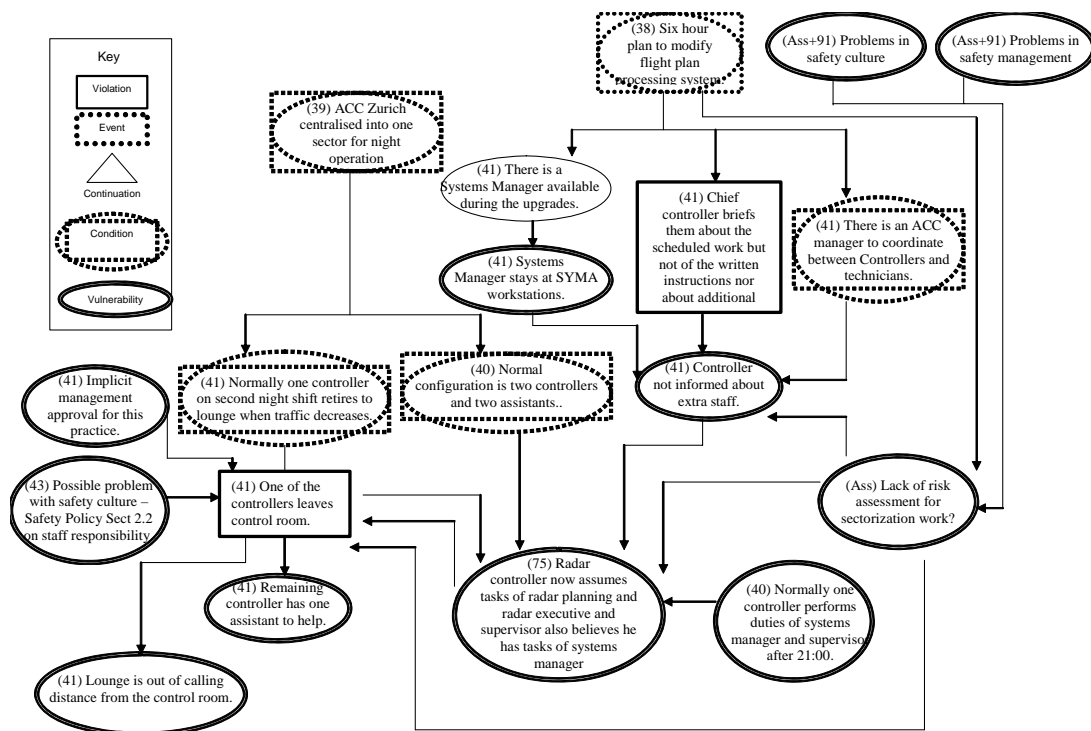


Figure 5: Immediate Factors Influencing the Technical Infrastructure in the Zurich ACC

Figure 5 continues our analysis and points to further common concerns between the Überlingen and Linate accidents. Staffing issues not only affected the response to the Linate accident, they also directly contributed to the Überlingen collision. The V2 diagram shows ACC Zurich’s normal configuration for night operations was based around two controllers supported by two assistants. It was also usual for one of the ATCOs to leave the control room and rest in the lounge as soon as the traffic died down. During the accident, one of the controllers left the control room. Management knew about this practice and there was no apparent pressure to stop it hence there was an assumption of at least implicit acceptance, documented on page 41 of the BFU report. The consequences of this practice were that the additional controller was now out of earshot from their remaining colleague. Meanwhile, the

six hour upgrade plan was also having an impact on the personnel and staffing of ACC Zurich. A systems manager (SYMA) was available to support the upgrade. However, they stayed at their workstation and controllers were unaware that this resource was available. Similarly, there was an additional manager to coordinate work between the technicians and the controllers. The Chief controller briefed his two colleagues about the work at the start of the shift but did not tell them about the additional staff. In consequence, a single controller was placed in a situation where they believed they were responsible for the tasks associated with radar planning, radar execution, shift supervisor and systems manager at a time when profound changes were being made to the technical infrastructure.

High Tolerance for the Loss of Computational Infrastructures

Figure 6 focuses more directly on the technological infrastructure at Linate. ATCOs had been provided with an analogue Aerodrome Surface Movement Indicator (ASMI) radar system. Traffic increases had exposed the reliability and low definition of this system to a point at which ATM personnel began to look for an alternative. There was a plan to introduce a NOVA 9000 Surface Movement Guidance and Control System (SMGCS) using video camera technology. The old AMSI system was, therefore, taken out of service three years before the accident. The plans to install the new system were jeopardized when the predecessor of ENAC (Italian Civil Aviation Authority) objected to the antenna location. They argued that this would involve additional expense by constructing a temporary structure that would then be moved once a new Tower was built. It was also argued that the proposed structure might hinder visibility and that there were few reported problems in handling ground traffic at Linate. The V2 diagram also illustrates the DGAC's concern that the new system would not harmonize with other European initiatives. This last point is particularly interesting as a reason to delay expenditure on a significant component of a ground-based infrastructure. It is counter-intuitive that ATM personnel would be deprived of an important tool so that the eventual system would be consistent with a European initiative that was intended to harmonize safety provision. It could be argued that this international safety initiative had the unintended effect of exposing the ATM personnel to greater risk. In July 2000, ENAV assumed many of the previous responsibilities held by DGAC. One side effect of this hand-over was that approval was finally granted for the development of the new Surface Movement Guidance and Control System. The antenna was to be located in the same position as the previous Aerodrome Surface Movement Indicator (ASMI) radar. The V2 diagram also shows that at the time of the project this upgrade project was further stalled as mothballed hardware had to be re-serviced before the new system could be delivered. As we have seen from Figure 4, the runway incursion sensors had already been deactivated on TWY R6. In consequence the ANSV argued that there was "no possibility" to confirm the positions of the various aircraft on the morning of the collision using technical aids [1].

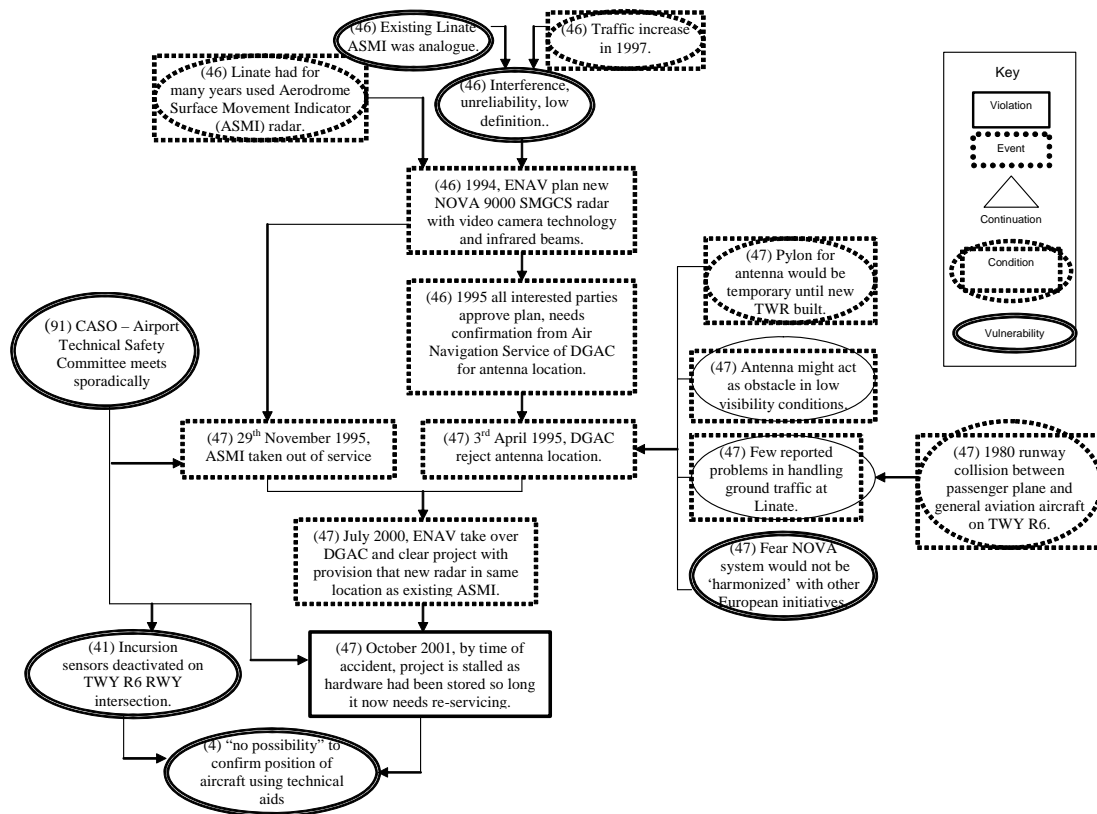


Figure 6: Technological Infrastructure at the Linate Accident

The RVSM related upgrades and maintenance operations had a considerable impact on the ATCOs in Zurich ACC during the Überlingen accident. Unlike Linate, these technical changes occurred in a much shorter period of time than the more gradual degradation of ground movement radar systems at Linate. However, there was a common failure to appreciate the impact that these changes had upon ANSP operational capabilities. The Zurich radar data processing system consisted of three main Thomson MV9800 computers. The first was used for primary operation, the second was held as a “hot standby”, the third was used for test purposes and software development. The system has a visual and acoustical STCA (Short Term Conflict Alert). If the connection between the MV9800 and the controller workstation system is interrupted, as it was on the night of the accident, then the correlated radar image is lost. Controllers must use the fallback radar computer (fbRDPS). This means that the controller must manually correlate radar targets with flight plans. The maintenance work that led to the loss of the MV9800-ICWS link also deprived the controller of the visual Short Term Conflict Alert, although an audible alarm was available. By forcing the manual correlation of radar targets and flight plans and by removing the prompt visual STCA warnings, the controller was placed in a vulnerable position. Figure 7 refers to the lack of documentation on the impact of the upgrades. It also links back to the lack of any adequate risk assessment and the impact that this may have had on, for instance, the Chief Controller’s briefing about the upgrade work.

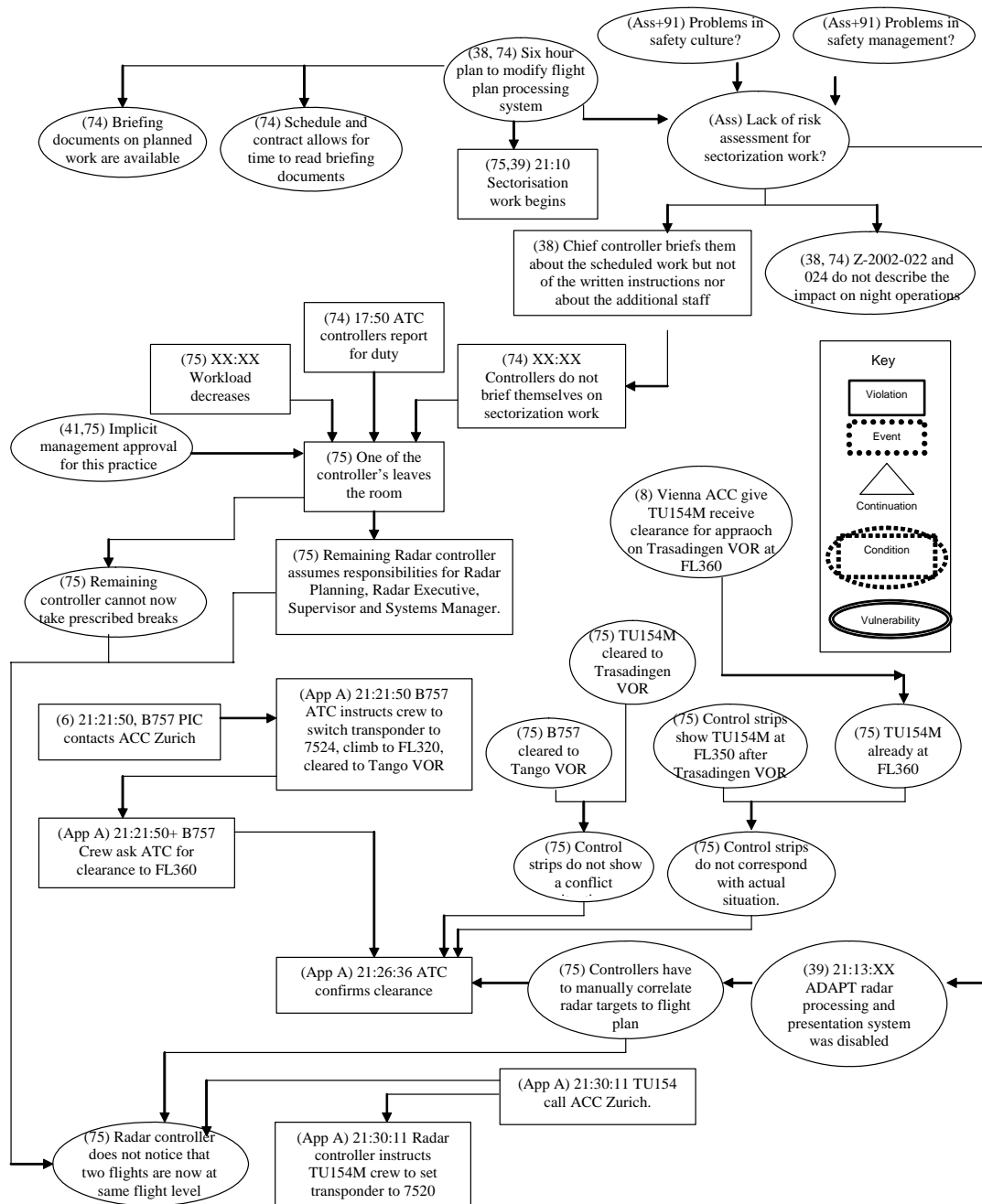


Figure 4: Technological Infrastructure during the Überlingen Accident

Conclusions

This paper has built upon the findings of official investigations to identify similarities between the Linate and Überlingen accidents. Both accidents had precursor events that might have warned managers of potential hazards. There were inadequate safety management systems for assessing the risks associated with particular working practices. In both cases, ATCOs were forced to cope with degraded technical infrastructures. However, both accidents also show that ATCO's will find 'work around' or 'make do' with degraded working environments. There are, of course, important differences between the two accidents. ATM personnel at Zurich were forced to cope with a relatively rapid degradation in their technical systems on the night of the accident. In contrast, the Linate ground controllers' faced prolonged periods without either Aerodrome Surface Movement Indicator radar or the proposed Surface Movement Guidance and Control system.

Inadequate risk assessment seems to have played an important role in both accidents. In the context of Linate, more sustained hazard analysis might have provided ATM personnel with additional information about the danger of runway incursions in low visibility conditions without the support of ground movement radar. Such a risk-based initiative could have been triggered by delays in the replacement of the former systems or by earlier runway incursions at Linate. Similarly, a more sustained risk analysis might have identified the importance of informing ATCOs about the impact that MV9800 upgrades would have upon their working environment.

Überlingen and Linate have implications beyond air traffic management. They provide lessons for the management of change in safety-critical infrastructures. Interaction between technical properties of the Überlingen LAN architecture and the social, working practices at Zurich ACC helped to create the context in which this accident occurred. Similarly, Linate stemmed from a complex combination of technical issues, including the gradual erosion of automated support, poor physical infrastructure, including obsolete taxiway markings, and communication failures between aircrew and ATCOs. In retrospect, many of the lessons are obvious. In particular, risk assessments for infrastructure maintenance must consider working practices, including single controller operations at Überlingen and procedures for mixed traffic at Linate, as well as the technical consequences of particular upgrades.

Many of the technical and organizational problems in these accidents can be traced back to inadequate safety management systems at Linate airport and within Skyguide. It can also be argued that these problems stemmed from fundamental tensions in the public policy provision for safety-critical infrastructures where semi-independent companies must meet strict financial targets and also provide social goods, including high levels of reliability. It is important not to underestimate the difficulty of creating and sustaining adequate safety management systems in organizations that are faced with market pressures and changing regulatory demands.

Biography

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads the Glasgow Accident Analysis Group, this small team of multi-disciplinary researchers is interested in understanding the role of computer applications in the failure of complex systems. He has held a NASA fellowship for his work on incident investigation techniques and helped to author incident reporting guidelines for European Air Traffic Management. He has published over 100 peer reviewed papers, including a Handbook of Accident and Incident Reporting that can be downloaded from his web site. He coordinated the EC ADVISES Research Training Network supporting human factors approaches to the design of safety-critical systems.

References

[1] Agenzia Nazionale per la Sicurezza del Volo (ANSV), Milano Linate, ground collision between Boeing MD-87, registration SE-DMA and Cessna 525-A, registration D-IEVX, Reference A/1/04, 20th January 2004.

[2] Bundesstelle für Flugunfalluntersuchung (BFU: German Federal Bureau of Aircraft Accidents Investigation), Accident on 1 July 2002, Near Überlingen/Lake Constance, Germany Involving Boeing B757-200 and Tupolev TU154M, Investigation Report AX001-1-2/02, May 2004.

[3] EUROCONTROL, European Action Plan for the Prevention of Runway Incursions, version 1.1, Brussels, Belgium, Available on: <http://www.eurocontrol.int/runwaysafety>, August 2004.

[4] Johnson, C.W., Establishing Public Policy as a Primary Cause of Engineering Failures in National Infrastructures. In C. Balducelli and S. Bologna, Proceedings of the ENEA International Workshop on Complex Networks and Infrastructure Protection, International Emergency Management Society", Rome, Italy, 2006.

[5] Johnson, C.W., A Handbook of Accident and Incident Report, Glasgow University Press, Glasgow, Scotland, 2003.

[6] Merckx, E., The SSAP European Strategic Safety Action Plan Implementation Programme: Monitoring the Safety of Europe's Sky, EUROCONTROL Summary document available on: <http://www.eurocontrol.int/ssap>.

[7] Reason, J. (1990) *Human Error*. Cambridge: University Press, Cambridge.

[8] van der Gees P.J., Piers, M.A., de Jong, H.H., Finger, M., Slater Acona, D.H., van Es, G.W.H., van der Nat, G.J., Aviation safety management in Switzerland: Recovering from the Myth of Perfection, Nationaal Lucht- en Ruimtevaartlaboratorium, National Aerospace Laboratory and the Swiss Federal Department of Environment, Traffic, Energy & Communication (DETEC), 2003. NLR-CR-2003-316, Available on: http://www.uvek.admin.ch/imperia/md/content/g_s_uvek2/d/verkehr/nlr/24.pdf