Understanding the Contribution of Degraded Modes of Operation as a Cause of Incidents and Accidents in Air Traffic Management

Christine Shea, PhD; ESR Technology Ltd, Birchwood Park, Warrington, Cheshire, UK.

Chris. W. Johnson, DPhil; Department of Computing Science, University of Glasgow, Scotland, UK.

Keywords: Air Traffic Management; degraded operations; accident analysis; organisational safety.

Abstract

This paper charts the role that 'degraded modes of operation' have played in a number of recent accidents and incidents in European Air Traffic Management. A central aim of this analysis is to begin to understand why teams of co-workers continue to operate safety critical systems even when key elements of their technological infrastructure have been compromised, for example during routine maintenance. There is often a culture of 'making do' where managers and staff try their best to maintain services. The extent to which workers will adapt to degraded modes illustrates the flexibility and resilience of socio-technical systems. However, it can also endanger safety when infrastructure changes act to increase workload or remove necessary 'safety nets'. It is hoped that by studying previous incidents and accidents, we may ultimately help operators and managers understand the dangers of degraded modes of operation while at the same time supporting the flexible working practices that are necessary in many complex, safety-critical systems.

Introduction

'Degraded Modes of Operation' have been a common feature in the causes of many recent accidents and incidents within European Air Traffic Management (ATM) [1]. The following pages focus on 3 case studies that have been chosen to illustrate the extent of these problems across several different nations. The Überlingen accident occurred on the 1st July 2002 when a Boeing 757-200 was involved in a mid-air collision with a Tupolev TU164M [2]. A total of 71 crew and passengers were killed on both aircraft. The immediate causes of the accident centred on the Air Traffic Control Officer's (ATCO) decision to instruct the Tupolev's crew to descend. This contradicted the Traffic Alert/Collision Avoidance System (TCAS) on-board warning system. The descent caused them to collide with the Boeing 757 which was also responding to a TCAS warning to avoid the Tupolev. The official BFU report into the accident provides a thorough analysis of the causes that led to the confusion over the warning from the TCAS software. In contrast, the following pages focus on the combination of latent failures and degraded modes of operation that affected the staff in the Zurich Air Traffic Control Centre.

The Linate accident happened on the 8th October 2001 when an MD-87 was taking off from runway 36R at Milan's Linate Airport [3]. The MD-87 collided with a Cessna 525-A, that had 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 working in a baggage handling building that was struck by the MD-87 immediately 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 went on to identify a number of organizational and technical limitations in the systems in the airport's operational environment that created the preconditions for the accident.

The final case study focuses on a collision between an MD-83 and a Shorts Brothers 330 aircraft at Paris' Charles de Gaulle airport [4]. The MD-83 was cleared for take off on runway 27, while the Shorts was then cleared to line up and wait as 'number two'. The BEA report argued that the controller believed both aircraft were at the threshold of the same runway and that the Shorts should, therefore, have waited for the MD-83. However, the Shorts had actually been cleared to use an intermediate taxiway and so entered the runway just as the MD-83, already moving down the runway for take off had reached rotation speed. The wing of the MD-83 entered the cockpit of the Shorts aircraft immediately killing the First Officer and leaving the Captain seriously injured. The accident report found that contributory factors included increased workload for operational staff at the time of the accident, light pollution which impeded visibility from runway maintenance operations as well as existing operational procedures and working methods.

What Are Degraded Modes?

It is difficult to-define a ‘degraded mode of operation’. Safety-critical systems that provide services over long periods of time, typically, suffer minor equipment failures. In consequence, most routinely operate for short periods of time with some form of ‘degraded’ functionality. In general, these faults are rectified without significantly endangering safety. However, there is usually an understanding that the risks associated with minor faults will only be tolerated for limited periods of time and will not affect core system functionality. Equally there are faults that are not rectified over many months and years. Operators and managers find ways of ‘making do’ without critical infrastructure. If a degraded mode is not addressed promptly over time it can become a latent weakness that eventually contributes to an accident or incident.

Operations managers are often required to develop corrective action plans that specify when and how faults will be managed. Minimum equipment lists (MEL) are also used. These enumerate core systems that must be provided in order for operations to continue safely. If periodic failures remove these applications then operations should cease. However, MELS are relatively inflexibile. The importance of specific safety-related applications cannot be determined without some knowledge of existing environmental conditions. To cope with this, organisations must draft a number of different MELs to address the different operating conditions that arise for complex systems in dynamic environments. For example, Linate airport operated under the procedures of the Italian Civil Aviation Authority (ENAC). These described those operations that could be conducted under different environmental conditions with particular support systems. In other words, the procedures were structured around MELs. For example, ENAV DOP 2/97 placed limits on the number of ground movements that were permitted under low visibility conditions if radio communications and ground movement radar systems are compromised [3, p.53]. In the Charles de Gaulle case study the use of an MEL allowed an aircraft to fly when it began to flag a failure on the ‘total temperature indicator’ Ram Air Temperature (RAT). The airline’s ‘MEL authorizes the flight under acceptable deferred defect conditions, providing the Engine Pressure Ratio limits are defined manually’ [4, p.34]. The operating company enforced this use of MELs under circumstances where Engine Pressure Ratio limits cannot be calculated accurately. Under other conditions it remains acceptable to defer maintenance using corrective action plans or ‘deferred defect conditions’.

MELs and corrective action plans are important elements in robust safety management systems (SMS). In recent years, SMS have been identified as an important means of protecting both operational and managerial staff from the commercial pressures that might otherwise undermine the safety of ATM operations. These systems typically use a risk-based approach intended to prioritise organisational resources to address those hazards that pose the greatest threat to operational safety by detecting potential problems, initiating corrective actions and monitoring the interventions [3, p.94]. They may also be used to initiate corrective actions against latent failures to increase resilience to degraded modes. Organisations such as ICAO provide guidance on the development of SMS in Annex 14 and EUROCONTROL advocates the development of SMS as detailed in ESARR3. However SMS and MELs require on-going support from management to be useful in the face of sustained commercial pressure to continue operations under adverse conditions. There is a strong link between an organisation’s ‘safety culture’ and the manner in which it preserves adequate safety margins during degraded mode operations. Conversely, the longer term acceptance of degraded modes of operation is often strongly related to deeper issues around safety management within complex organisations. The influence of organisational factors on daily ATM performance cannot be underestimated at. Operational staff, including ATCOs and pilots, must juggle the commercial requirements to maintain or improve performance levels while maintaining high levels of safety.

Management of Environmental/Meteorological Conditions

There are often vulnerabilities in complex systems that otherwise appear to make adequate provision for safe operations. These vulnerabilities are revealed when the system is under pressure, for example in poor meteorological conditions. This is illustrated by the Linate runway incursion [3, p.162]. The ANSV identified a number of causes linked to mismanagement during poor meteorological conditions, including the “operational procedures allowing high traffic volume in [poor] weather conditions … and in the absence of technical aids” [3, p.163]. Neither the Cessna nor its pilots were qualified to take-off under the Cat II/III conditions that held during the accident. ATM personnel cleared them for take off, nevertheless. The ANSV provide an implicit analysis of the pressures that might have shaped the crew’s decision. These included personal and commercial incentives to complete the flight. In the Charles De Gaulle case study, poor visibility degraded operating conditions and exposed vulnerabilities in the underlying safety systems. “Visual surveillance of the manoeuvring area around the threshold of runway 27 was very difficult to perform. It was dark, the rain had made the ground reflective and the lighted area of the work-site was located between the north tower and threshold 27” [4, p.48].

The Role of Safety Management Systems and Safety Culture

The ANSV and BFU investigations into Linate and Überlingen illustrated the important role that Safety Management Systems play in an effective response to degraded modes of operation. The BFU observe that a “SMS and associated management systems are potentially effective tools an organization can use to influence the safety culture and support the stated priority of safe air navigation. A lasting behavioural change in individuals based on changes in personal attitudes takes a certain amount of time even with a well-structured and well-founded safety system” [2, p.90] These links were also emphasized when analysing the organizational structures intended to manage safety related changes within Skyguide, the Air Navigation Service Provider, and Zurich control center prior to the accident. Skyguide faced a time of change as deregulation and market pressures were increasingly being applied to their operations. The safety policy of the company had been redrafted a short time before the accident and embodied many of the safety management principles proposed by ICAO and EUROCONTROL. However, there were many practical problems associated with its implementation. A Centre of Competence was, therefore, created to coordinate necessary improvements, for example in risk assessment and the development of safety monitoring functions. In particular, the organisation only had limited experience of risk based approaches to system development and maintenance. The necessary skill base had to either be bought-in from outside or developed by providing appropriate training and experience to existing personnel. The BFU record that the ANSP “elected to develop these systems themselves rather than bring in the expertise from outside the organization” [2, p.91]. There was a delay while these skills were built up. The lack of trained and experienced safety managers also placed considerable demands on the existing personnel. The BFU report argues that the Centre of Competence should have been formally involved in the infrastructure changes at ACC Zurich that contributed to the accident, according to the Safety Management provisions of the Safety Policy. However, this did not happen and without any further indication of the nature of the planned maintenance work there was little prospect that Skyguide’s Risk Manager would become involved in a formal risk analysis of the upgrades [2, pp.90-91].

As mentioned, the Linate report criticised the lack of Safety Management Systems before the incursion reviewed in this paper. The ANSV stated that the accident was caused in part because “no functional Safety Management System was in operation” [3, p.163]. The reasons for this have some similarity with problems that were identified in the aftermath of the Überlingen accident [1]. These related to the problems of implementing risk-based design and maintenance across complex organizational structures under increasing pressures for deregulation and competition within the aviation industry. A large number of organizations, including ENAC, the SEA, CAV, DCA etc, all contributed to or influenced the CASO, Airport Technical Safety Committee. Partly in consequence, this group was only able to meet sporadically. This creates a circular argument. The failure of the CASO to review the technical aspects of safety policy was in part due to the lack of an effective Safety Management System. Conversely, the failure to develop Safety Management Systems stemmed in part from the lack of effective tactical input from these technical subcommittees who might otherwise have been pushing for additional strategic guidance from higher levels of management. The lack of a fully-developed Safety Management System may also have contributed to the absence of a runway safety plan. The absence of a runway safety team also made it difficult to identify all of the groups who were responsible for ensuring compliance with ICAO runway requirements. The key insight here is that managerial and organisational structures have a critical role to play in detecting and responding to longer term problems associated with degraded modes of operation.

Degraded Operating Procedures

Degraded modes of operation can also refer to changes in operating practices, including failure to follow standard operating procedures. For example, the BEA contrast the recommended procedures and phraseology for handling taxiing aircraft with the steps taken and phraseology used prior to the Charles de Gaulle incursion. For taxiing to a holding point the operations manual states that “In paragraph 4.7.1, *Line-up from high speed exit (DGV)*, the manual indicates that line-up from a DGV is possible only if the RVR is over eight hundred metres and the ceiling over three hundred feet. In this case: *subject to acceptance by the crew and after co-ordination with LOC control, the aircraft is guided to the required taxiway. The taxiway number is indicated in the strip*... It should be noted that the phraseology does not require systematic association of the taxiing instruction with the taxiway allocated” [4, p.30].

A contrast is drawn between these documented procedures and the interaction between the controller and the crew of the Shorts aircraft. During taxiing, the ATCO asked the aircrew if they wished to take off from an intermediate access taxiway given the short take-off ability of their aircraft. The crew requested departure via taxiway 16 and the ground controller replied with the non-standard phraseology *"That's fine, so one six is approved, Streamline two hundred"*. The use of such informal clearances is also illustrated in the use of 'line up' in sequence instructions prior to the Charles de Gaulle incursion. ATCOs can authorise aircraft to line up behind another departing plane. These clearances are, typically, issues once the aircraft reaches a holding point. Pilots can then enter the runway at their own discretion after the previous aircraft has taken off. 'Line up' clearances reduce the workload on controllers because they avoid some of the tasks associated with line-up management. However, they are not mentioned in the national and international reference texts. There are obvious concerns over the consequences of any confusion in issuing or receiving line up clearances. As the BEA note, "the aircraft scheduled for departure after the Shorts received an in sequence line-up instruction some ten seconds before the collision: *Eurotrans 9263, line up in sequence, number 3"* [4, p.30].

A variety of different procedural violations were identified in the aftermath of the Linate runway incursion. There are similarities with the problems identified by the BEA following the accident at Charles de Gaulle. For example, the report concluded that "radio communications were not performed using standard phraseology (read back) or were not consistently adhered to (resulting in untraced misunderstandings in relevant radio communications)" [3, p.163]. Many of the phraseology problems stemmed from ambiguity between the clearances that were issued so that it was difficult, if not impossible, for aircrews to determine whether they related to taxiway R5 or R6. This, in turn, made it difficult for the Cessna's crew to identify that they had chosen the wrong direction at the junction point of these two routes. The ANSV argued that "the words *report the stops, report the bars, report at the stop bars*, have been used both in clearances involving TWY R5 and TWY R6, without any other clarification or identification of the route to be followed" [3, p.114]. It is important to stress that aircrews were complicit in the failure to follow approved procedures. An analysis of communications on a single radio frequency at Linate involving traffic on the West apron during the 2 days prior to the collision, revealed 7 instances where the aircrews failed to read back part of the clearance that had been issued. There were four instances where the clearances were entirely missing from the read back. Some of these informal practices emerged as strategies to help ATCOs and flight crew cope with problems in the operational environment. However, they also created an ambiguity and imprecision in communication that exacerbated the problems associated with degraded operations prior to the accidents.

The Linate accident also shows that inappropriate Standard Operating Procedures (SOPs) threaten safety by permitting degraded modes of operation. The ANSV recognized that the accident was partly caused by "operational procedures allowing high traffic volume (high number of ground movements) in weather conditions as were current the day of the accident (reduced visibility) and in the absence of technical aids" [3, p.163]. It can be argued that inappropriate procedures might have been challenged by a risk based approach that underpins many Safety Management Systems. A more thorough analysis of the hazards associated with operating under such adverse conditions might have alerted operational and management staff to the potential risks of runway collisions under these degraded modes of operation.

The Überlingen accident provides examples of rules and procedures that did little to support operational staff. The BFU identified one of the systemic causes of the mid-air collision as "The regulations concerning ACAS/TCAS published by ICAO and as a result the regulations of national aviation authorities, operations and procedural instructions of the TCAS manufacturer and the operators were not standardised, incomplete and partially contradictory" [2, p.4]. ACAS refers to Airborne Collision Avoidance System and has been adopted by the ICAO in contrast to the term TCAS, which is in more general usage in the United States. For example, the ICAO Procedure for Air Navigation Services – Aircraft Operations, Volume I, Flight Procedures (Doc 8186, PANS-OPS) contains a section on the 'Operation of ACAS Equipment'. The requirements in this document have been described as 'insufficient and unclear' [2, p.79]. The ICAO guidance contains the statement that ACAS 'assists' pilots and that "*Nothing in the procedures shall prevent pilots-in command from exercising their best judgment and full authority in the choice of the course of action to resolve a traffic conflict*". This contradicts the TCAS system philosophy embodied within the TCAS 2000/TCAS II Traffic Collision and Avoidance System Pilots Guide [2, p.53].

The Überlingen accident also illustrates the way in which procedures and regulations can be difficult to apply during degraded modes of operation. ICAO Procedures for Air Navigation Services - B Air Traffic Management, known as

Doc 4444, PANS-ATM states that controllers must not issue instructions to alter that path of an aircraft when the aircrew reports a TCAS resolution advisory until the conflict has been resolved. This guidance could not be applied to the Überlingen accident because the crew of the TU-154M did not inform the ATCO of the advisory nor was there any automated system to provide such information to him (BFU, 2004, p.79). Further inconsistencies can be identified between, for instance, the TU-154M flight operations manual and the ANSP documentation covering TCAS advisories. Rules and regulations clearly failed to help avert our case study incidents. The plethora of contradictory or ambiguous guidelines on the operation of TCAS was not readily usable to support the ATCO - even if he had been aware of their different nuances and requirements.

Staffing and Competence Levels

Competency and staffing levels are generic factors that may undermine ATCO performance during degraded modes of operation. The use of one controller in the Zurich ACC at the time of the Überlingen mid-air collision was an unofficial practice, however, the BFU report acknowledges that "this way of proceeding which does not provide any redundancy of human resources so that procedural errors, wrong distributions of attention or the omission of important actions may lead to hazardous situations as nobody is there to notice these mistakes and to take corrective actions… Even though it was an unofficial procedure it was known to and tolerated by the management" [2, p.75]. The second controller left ACC Zurich after air traffic volume had decreased. Normally he would have returned to the control room as workload increased with early morning air traffic. The remaining controller was out of earshot of the second controller resting in the lounge. He then had to perform the tasks normally associated with the Radar Planner (RP) and Radar Executive (RE) as well as the Chief Controller. Although he did have a Controller Assistant to support this work, she had no rating for Air Traffic Management [2, p.41].

It is always important to consider such observations in the context of the environment that faced operational staff at the time of the accident. A control room designed for operation by greater numbers of staff could only ever be run in a 'degraded mode' by such a small number of controllers. This is illustrated by the Controller having to divide his attention between different areas of the control room since a workstation on the left was intended for the Radar Planner and presented all of the ACC Zurich airspace while a workstation on his right was dedicated to the Radar Executive. The controller used this to select a more detailed view of the sector for the approach to Friedrichshafen airport and switched the radio system to the frequency appropriate for movements in this area. This terminal could provide a view of the aircraft involved in the eventual collision. However, in order to contact them on their radio frequencies it was necessary for him to move to another workstation [2, pp.41-42]. The demands of these various tasks and the consequent disruption caused by moving between the different positions played a significant part in undermining his situation awareness. The loss of situation awareness, in turn, impaired his decision making ability during key stages of the accident.

The causes of insufficient or inadequate staffing levels and competency are specific to the particular circumstances of each accident. For example, the Tower Controller on duty during the incursion at Charles de Gaulle airport was an instructor at ENAC (National Civil Aviation College). As part of the requirements for this role, he had to maintain his operational qualifications by spending time as a controller. The BEA note that "irrespective of the duration of their absence, no procedure for instructor controllers in-service adaptation is envisaged, due to their role as instructor, which keeps them in permanent contact with ATC" [4, p.33]. There has never been an instance in which a controller was unable to perform the duties assigned to them and maintain their qualifications. However; "Instructors undergoing qualification maintenance generally generate additional workload for the instruction divisions of the centres. Instructors have also complained on some occasions of not being considered as an integral part of the team" [4, p.42]. The integration of instructor controllers into operational teams provide insights into the specific events that led to the accident. The head of the airport's Air Traffic Management division was also in the tower at the time of the accident. He was there to help manage the workload associated with additional flights that had been scheduled to carry the fans attending an international soccer match. This manager began placing strips directly on the control board of the instructor controller. In most circumstances, the strips would have been placed on the side of the board to enable the ATCO to integrate them himself after considering possible conflicts. By placing the strips directly on the board, the head of ATC may have removed a further check for potential conflicts performed by the controller [4, p.40]. The status of the instructor controller as a 'guest' within the tower, may have given rise to social and cultural barriers preventing him from objecting to his colleague's actions.

Mixed Mode Operations

'Mixed mode' operations describe the integration of commercial and general aviation on the same taxiways and runways. This integration forces ATCOs to integrate aircraft with very different performance characteristics on the same infrastructure. It also creates specific demands on operational staff that can be difficult to sustain during degraded modes of operation. Immediately after the Second World War, Linate used separate runways to handle both general and commercial aviation. This simplified Air Traffic Management. Subsequent developments opened up access for general aviation to runway 18L/36R which had previously been reserved for commercial operations. This did not significantly increase controllers' workload because of the relatively small scale of general aviation at this time. Partly in consequence, a culture of familiarity grew up between ATCOs and pilots. Over time, the performance of general aviation aircraft began to match that of commercial aviation and the demand from general aviation to use 18L/36R also increased. The airport did not develop any high level plan to deal with these changes. In consequence, ATCOs had to act as a buffer. They developed working practices and coping strategies that enabled them to continue service provision for a very diverse range of aircraft operating on 18L/36R [3, p.30].

Similar comments can be made about the emerging situation at Charles de Gaulle. In this case, Streamline Aviation developed a freight transport operation using aircraft that only needed a short runway length to take off. Therefore, it was usual for the crews to take off from an intermediate access taxiway at Paris Charles de Gaulle. Controllers had to monitor aircraft entering the runway at different points depending on their takeoff requirements, just as they did at Linate [4, p.34]. The key point here is that 'mixed mode' operations place additional demands on operational personnel that can act as a trigger to the longer term, or latent problems, that can exist within the ATM working environment. The mix of aircraft performance levels using the same areas of an airport need not necessarily create any operational problems. However, when it is combined with degraded operations including poor visibility and inadequate runway signage, these mixed operations are likely to play a significant factor in runway incursions.

Lack of Organisational Response to Precursor Incidents

The events leading to the Charles De Gaulle runway incursion shared much in common with an airprox incident that had occurred shortly before the accident. This prompted an extensive review, which addressed "development of pilots' and controllers' awareness of the parallel runway characteristics and the specific management of runway crossing, via the production of a widely distributed video; creation of the Prevention and Safety Group; acquisition of a high performance runway control simulator providing 360° viewing capability, and implementation of an intensive training programme for the controllers; transfer of South LOC position to the South Tower for improved visibility; installation of a second "ASTRE 2000" ground radar in the South Tower, to supplement the radar already installed in the North Tower" [4, p.36]. However, the adequacy of these measures was not reviewed when a second airprox incident took place. These incidents reveal that crucial safety concerns had been acknowledged - even under near optimal conditions. However, there was no systematic attempt to ensure that these concerns were monitored in the months leading up to the accident.

Two previous airproxes had occurred at ACC Zurich during Single Manned Operation Procedures (SMOP) which had emerged informally over time. Ultimately, a single ATCO was left at his post while his colleague took a break; though this informal practice was never approved for night operations and SMOP guidance was only developed for use during daytime shifts. However, two previous incidents had already led the Swiss BFU and BAZL to raise questions about these operations [2]. ACC Zurich defended their practice by stating it was common in other European states. Similar to the Charles De Gaulle incident, no formal review was used to assess the acceptability of current or future practice though it appears that the ANSP felt that SMOP was an unacceptable operating mode in the long term. The problems of SMOP were exacerbated by the degraded modes of operation that persisted at the time of the accident. As noted in the BFU's official report 'The radar system was being operated in the fallback mode and the optical Short Term Conflict Alert was not available; the telephone system was not working properly; the technicians working in the control room added to the controller's stress; operating two workstations with two different sectors from radar screens set to different scales was an additional strain and would probably not have been accepted by a supervisor although traffic flow was low; the ATCO could not use a headset as he was operating radios of two workstations. The regulatory authority had already voiced concern about SMOP. The general work conditions during the night shift and the additional strains of the night of the accident did not meet the requirements for SMOP" [2, p.92].

The Italian ANSV lists 4 similar incidents prior to the Linate runway collision. One occurred only 24 hours before the collision; an aircraft taxied along TWY R5 instead of R6 and the Controller was only alerted to the incident when the crew realized their mistake. These incidents were caused, in part, by the degraded state of the runway and taxiway infrastructure. Inconsistent signage created problems for aircrews navigating onto appropriate runways. Further problems arose because ATCOs could no longer alter the configuration of runway and taxiway lights to provide positional cues to aircrew. Over time many of the deficiencies had become 'normal' practice. The warnings provided by the previous adverse incidents about the potential consequences of these latent failures, particularly when combined with the degraded 'low visibility' operations that held at the time of the accident may have prevented the accident but only if warnings were being heeded.

Organisational Management of Degraded Modes across Functional Boundaries

The operational shortcomings of ATM systems in each of our case studies are only part of a wider picture of suboptimal systems. Aircrew often cope with partial system failures while ATCOs find 'work arounds' to manage inadequate infrastructure. In the Charles De Gaulle incident, limitations with the ASTRE radar system may have prevented the controllers from identifying the Shorts as it approached the runway. At the same time, the crew of the MD83 were struggling to resolve a Ram Air Temperature warning. The Cockpit Voice Recorder indicates that this failure made it impossible to use the automatic throttle and consumed finite resources of time and attention in the moments before the accident. [4, p.20]. The same latent, infrastructure issues hindered ATCOs and aircrew in the Linate incident. The use of inconsistent signs and inadequate control over runway and taxiway lighting impeded both controllers' and pilots' ability to identify the precise locations of the aircraft. The "lack of position, direction, location signs and proper markings on the West apron were three factors that made situation awareness for the Cessna crew difficult [3, pp.106-7].

In contrast the Traffic Collision Avoidance System (TCAS) worked 'flawlessly' on both the TU154M and the B757 in the Überlingen accident [2]. The problems did not result from any malfunction in the TCAS system. They stemmed from the interaction between the ATCO, whose working situation was degraded, and the actions taken by the crew of the B757, who obeyed the ATCO and ignored the automated advisories from TCAS. The system correctly issued advisories for TU154M to climb and for the B757 to descend. However, the TU154M crew followed the ATC instruction to descend and continued to do so even after TCAS advised them to climb [2, p.112]. The official investigation noted that "TCAS only makes sense if worldwide all crews rely on the system and comply with the advisories...The crew must comply with the RA without delay and report the initiated TCAS manoeuvre to the controller. Any other procedure which does not sufficiently take into account the priority of an RA would be contradictory to the purpose of TCAS" [2, p.77]. Subsequent changes to the TCAS system arguably provide valuable insights into design issues that weakened or degraded previous versions of these applications. For instance, recent versions of TCAS generate 'Reversal Resolution Advisories'. These change the direction of the initial advisory as further information is obtained about the likely position of any other aircraft involved in a conflict.

Workload

Workload can be defined in terms of the demands or load placed on a person's cognitive processing abilities [5]. It can significantly influence how efficiently and effectively individuals process information and make decisions. As Lichacz noted in his study of the effects of combined stressors on dynamic task performance 'ATC performance was susceptible to the effects of time pressure and workload' [6]. Traffic complexity and volume also had an impact. A review of our incidents suggests that workload may have been a contributory factor in each case and was exacerbated by the degraded modes of operation. At the time of the Linate collision, visibility was reduced to between 50 and 100 meters and workload was high; '…in the 16 minutes from the time that the MD-87 requested taxi clearance to the collision, the GND controller managed 126 radio communications. [and] The TWR controller managed 73 radio communications [3, p.28]. There was no possibility of using technical means to verify the position of these aircraft and several messages were relayed to each crew during this interval. This combination of traffic density, poor technical infrastructure and meteorological conditions created a 'demanding' environment for the ATCOs [3, p.4].

Immediately before the Charles De Gaulle runway incursion the controllers were under considerable pressure. Additional flights were scheduled to carry rival supports attending a soccer final between Madrid and Valencia in Paris [4, p.27]. A number of measures had been introduced to ease the additional workload on staff. These included using three runways; increasing the number of controllers and setting up a special operations centre. An engineer was provided on "standby" to the controllers and another liaised between the tower and the special operations centre to identify any flights that might be delayed [4, p.27]. The ATCO was experienced and an Ecole Nationale de l'Aviation Civile (National Civil Aviation School) instructor. However, he had not been in active service for five months prior to the incident. The ATCO had to re-familiarise himself with practice and procedures following a significant time away from active duty and was having to move between the cognitive demands of knowledge and rule based processing [7]. He was also having to consider the impact of construction work, such as the use of an intermediate access taxiway. In addition, he lacked information required to make accurate and efficient decisions due to the 'garbling' and poor radar images available from the ASTRE system. The more sophisticated AVISO radar screen was inaccessible without recourse to visual monitoring due to light pollution from the construction work; 'ASTRE (situated on the right-hand side of the combined station) presents only primary radar targets i.e. without identifying them and AVISO which presents a synthetic colour image of the traffic and the identity of aircraft and other vehicles on the runways and taxiways. The more useful AVISO radar screen was not accessible due to its distant location as only the ground control positions are AVISO equipped. On the more accessible ASTRE radar screen there were many fixed and mobile plots within and around the work area, with a lot of garbling also on the whole image' [4, p.38].

Increasing levels of workload also affected the ATCO prior to the Überlingen accident. The demands on the ATCO were again greater than average, typifying many aspects of degraded operations. Under normal conditions i.e. with at least one other ATCO working alongside him, the demands could have been shared. The BFU note 'With regular monitoring of the upper air situation as presented on the radar screen the conflict between the two aircraft at FL360 should have become evident to the ATCO. However, as the situation deteriorated the controller's workload increased subtly and continuously, reducing his ability to maintain an awareness of the upper air situation and be proactive in its control.' [2, p.85] This finding emphasises not only the increased demands on the ATCO but also the most challenging aspect of workload; how to assist an individual in recognising when it may become too much.

Communication Issues

Numerous hazards arise when operational staff, managers and maintenance teams fail to communicate that particular safety features are unavailable. It can be difficult for the members of these different groups to accurately convey their tasks and priorities to co-workers who have little experience or understanding of their different activities. These communication problems are compounded when both operational staff and maintenance teams are unaware of and/or do not appreciate their significance for each other as they attempt to operate and manage degraded operating modes. For example, the Überlingen report described how the controller on duty 'had not been informed' about the presence of an additional manager who was supposed to act as a 'coordinator between controllers and technicians'. Nor was the ATCO informed of a systems administrator added to the roster to support operational staff during the maintenance procedures on the night of the accident. [2, p.39]. Neither the manager nor the systems administrator were mentioned in the directives documenting the work that was taking place at the time of the collision.

During the Charles De Gaulle accident, communications problems arose over the maintenance activities that were scheduled. Testimony from the Tower Controller indicated that he had "formed a picture of the situation based on a false hypothesis: the fact that, because of the works, taxiways 16 and 17 would not be in use. For him, departures were to take place from the runway threshold" [4, p.45]. This erroneous perception was perpetuated by the lack of any integrated briefing between the maintenance managers and the tower team which might have helped to ensure that all controllers shared a common understanding of the impact of subsequent maintenance and may have created greater resilience to degraded modes of operation. Aircrews have also struggled to access documentation intended to provide warnings about latent failures and degraded modes of operation. The building work for the new North dual runways at Charles De Gaulle was explicitly mentioned in NOTAM No. 109/99. Additional information was provided regularly by the Aéroports De Paris via the Aeronautical fixed telecommunication network to airline staff present at the airport including updates of the list of taxiways that were closed. These were not passed to the Air Liberté (MD83) and Streamline (Shorts) crews because they do not have permanent staff at Charles De Gaulle. Nor did they access it using the Automatic Terminal Information Service which provided information about the closed taxiways that were updated by the Ground subdivision and approved by the Control unit each day. On the night of the accident, taxiways 16.1, 17.1, 17 and HP1 were closed. Runway threshold 27 was served by lanes B2, B1, 18.2 and 18.1, and Q. From 20:30 until 04:30, approximately ten vehicles worked on the site using orange emergency lights with high-power halogen lamps [4, p.18-19]. This information might have helped orient the crew as they manoeuvred around the open taxiways in response to the ATCOs' guidance.

At Linate, there was a similar breakdown in communication between the groups responsible for the maintenance of the infrastructure and the operational staff. The gradual degradation of taxiway signage, the loss of critical runway lighting systems and the failure to update the analogue ground movement system gradually removed critical infrastructure support from the ATCOs. The ANSV investigators found that these latent failures exacerbated the degraded operating modes under reduced visibility finding it 'remarkable' that the radar and lighting systems had not been improved in the months and years before the accident [3, p.107]. Such observations are symptomatic of a breakdown in communication between maintenance management and teams of operational staff who must continue to maintain levels of safe service in the face of latent failures. Communications failures often exacerbate degraded modes of operation, for example, if staff are not told about short term problems with key infrastructure. Our case studies provide evidence that operational staff may either not have studied or acted upon documentation describing infrastructure problems. More senior management must actively reinforce good practice. At Linate it was particularly difficult for aircrews to use existing documentation to gain an accurate understanding of the operational environment. Crucial markings particularly between taxiways R5 and R6 were indicated by yellow signs indicating the name of each route and by lines leading in the appropriate directions. However, there were no other indications between the bifurcation of R6 and the intersection with runway 18L/36R. The yellow line indicating the path of the taxiway had also been partially obscured by black paint that had been used to cover an old path that had been modified. In consequence, the Jeppesen charts used by the crews did not provide accurate information about the state of the taxiways [1, p.34]. The official investigation argued that the lack of information about the taxiway signage may have adversely affected the situation awareness of the Cessna's crew [1, p.119]. The ICAO Aerodrome Design Manuals provide guidance on the correct markings to use in these circumstances, and there is an obligation to ensure that any changes in runway signage are reflected in the documentation that is made available both to ATCOs and aircrews to ensure safe air traffic management. If such information is not provided then it is little surprise that crews and ATCOs are ill prepared to face the additional demands under degraded modes of operation.

Conclusions

Degraded modes of operation have played a significant role in recent Air Traffic Management accidents. Teams of co-workers continue to operate safety critical systems even when key elements of their technological infrastructure have been compromised, for example during routine maintenance. There is often a culture of 'making do' where managers and employees try their best to maintain services. The extent to which workers will adapt to degraded modes illustrates the flexibility and resilience of socio-technical systems. However, as we have seen this can also undermine safety when infrastructure changes subtly but steadily increase workload and impair necessary 'safety nets'. By studying previous incidents and accidents, we can help staff and managers to understand the dangers that they face from degraded modes of operation.

The three case studies presented in this paper provide an initial study of the hazards that are posed by degraded modes of operation. Further work is required to better understand the coping strategies and mechanisms that ATCOs rely on to manage increasing levels of demand. Consideration must be given to the resilient support mechanisms developed when degraded modes of operation are created by resource limitations, including lack of financial support and limited access to experienced safety managers. Improved implementation and use of incident reporting systems may help to shed light on the positive efforts to address infrastructure failures. However, additional studies are needed to elicit information about those instances in which ANSPs successfully dealt with degraded modes without endangering safe and successful operations. Our case studies relate to incidents involving Swiss, Italian and French ANSPs. They demonstrate that degraded operations can lead to accidents in organisations that have a significant history of safe and reliable service provision. Future work will consider whether degraded modes create acute problems for established organisations in contrast to developing states with less investment in legacy systems. If this hypothesis is correct then service providers in Europe and North America will have the most to learn from studying accidents involving degraded modes of operation.

Acknowledgements

We would like to thank Tony Licu, Paul Humphreys and Olivier Ferrante for providing valuable feedback on an early draft of this paper.

References

1. Johnson, C.W. (2006), Linate and Überlingen: Understanding the Role that Public Policy Plays in the Failure of Air Traffic Management Systems. In C. Balducelli and S. Bologna (eds.) Proceedings of the ENEA International Workshop on Complex Networks and Infrastructure Protection, International Emergency Management Society/Italian National Agency for New Technologies, Energy and the Environment, 508-519, Rome, Italy.

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

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

4. Bureau Enquêtes-Accidents (BEA: Accident Investigation Agency, June 2001), Accident on 25 May 2000 at Paris Charles de Gaulle to aircraft F-GHED operated by Air Liberté and G-SSWN operated by Streamline Aviation, Investigation report F-GHED/G-SSWN - 25 MAI 2000.

5. Endsley, M.R. and Smolensky, M. W. (1998) Situtation awareness in air traffic control: The picture. In E.S. Stein and M.W. Smolensky (Eds.) Human factors in air traffic control. San Diego, CA: Academic Press

6. Lichacz, F.M.J, (2005) 'Examining the Effects of Combined Stressors on Dynamic Task Performance' in International Journal of Aviation Psychology, Vol. 15, No. 1, pgs. 45-66.

7. Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man and Cybernetics*, SMC-13: 257--266.

Biography

Christine Shea, M Ed, PhD, ESR Technology Ltd, Whittle House, Birchwood Park, Warrington, Cheshire, WA3 6FW. E-mail - christine.shea@esrtechnology.com

Christine Shea is a principal consultant in safety and risk management with ESR Technology. Her work involves the management of risk in complex, safety-critical domains including aviation, rail, the petroleum industry and health care. Her research interests include the management and organisation of work in safety critical domains, safety culture, the development and implementation of incident reporting systems and human error.

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.