A Comparison of the Role of Degraded Modes of Operation in the Causes of Accidents in Rail and Air Traffic Management

Chris. W. Johnson* and Christine Shea†,

* Department of Computing Science, University of Glasgow, Scotland, UK, Johnson@dcs.gla.ac.uk
† ESR Technology Ltd, Birchwood Park, Warrington, Cheshire, UK, christine.shea@esrtechnology.com.

Keywords: railways; Air Traffic Management; accident analysis.

Abstract

Degraded modes of operation occur when technological systems fail to meet the levels of service that are expected by staff and managers. Over time, operators develop 'work arounds' that help them to cope with these degraded modes. This has led to a culture of 'making do' where co-workers try their best to maintain service provision in spite of system failures. The extent to which operators will adapt to degraded modes illustrates the flexibility and resilience of socio-technical systems. However, these adaptations and 'work arounds' undermine safety. A central aim of this paper is to begin to identify why teams of co-workers continue to operate safety critical systems when key elements of their infrastructure have been compromised, for example during routine maintenance. The following pages build on four case study accidents from the rail and air traffic management domains.

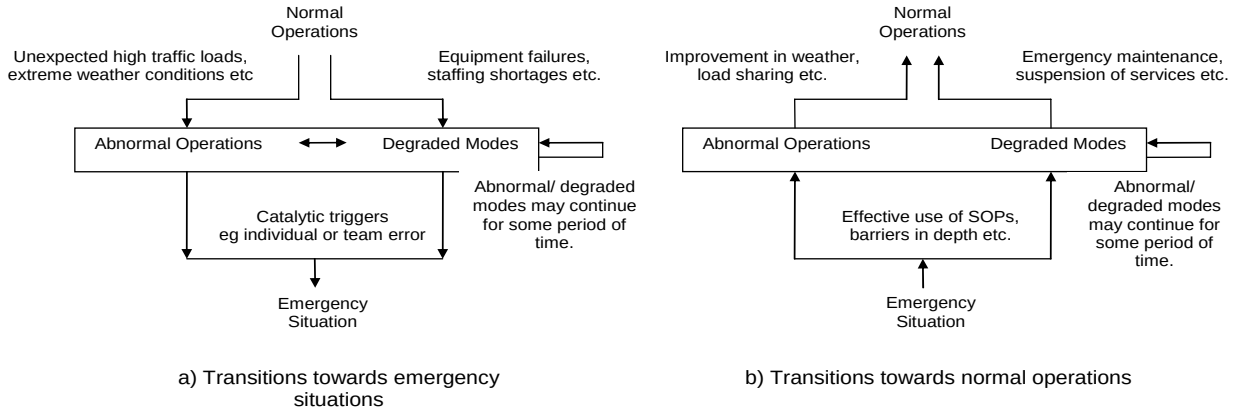
1. Introduction

Recent accidents in the air traffic management and rail transportation domains have occurred during 'degraded modes of operation'. This term describes the situation when complex systems continue to be operated without key elements of the supporting infrastructure. The extent to which workers will adapt to degraded modes illustrates the flexibility and resilience of socio-technical systems. However, by studying previous incidents and accidents we may help operators and safety managers begin to recognize and understand when and why degraded modes of operation become unsafe.

A secondary aim of the paper is to raise questions about the role of risk assessment techniques as a means of guarding against degraded mode failures. It can be difficult to apply many existing tools given the integrated nature of air traffic management and railway operations, the blend of leading-edge and legacy systems, the scale of interacting components. The incidents examined in this paper show great inconsistencies in the application of these techniques. The successful application of quantitative techniques, typically, depends upon the skill and expertise of the analyst. These vary greatly even within the same organisation. These problems are compounded because risk assessment techniques cannot, typically, predict all of the ways in which complex systems can fail. In particular, the following pages will show how these techniques often fail to anticipate the workarounds that characterize degraded modes of operation.

2. What Are Degraded Modes?

Degraded modes deprive operators of elements in the supporting infrastructure that are otherwise available under 'normal' conditions. The UK Railway Group Standards [1] contains the following distinctions. **Normal operations** describe the way in which the railway was designed to operate, including planned peak periods. **Abnormal operations** arise from extreme loading on a part of the railway system, for example as a result of severe weather, or delays to a train service impinging on others. **Degraded operations** occur when part of the railway system continues to operate in a restricted manner, for example after the failure of signals. **Emergency situations** include an unforeseen or unplanned event which has life-threatening or extreme loss implications and requires immediate attention, for example a fire, or an obstruction on a line. Figure 1 illustrates key relationships between these different modes of operation.



a) Transitions towards emergency situations

b) Transitions towards normal operations

Figure 1 — Overview of Degraded Modes in the Transition to Emergency Situations

The following pages focus on four case studies from two different domains. The Glenbrook collision occurred in New South Wales, Australia [2]. An interurban passenger train collided with the rear of an Indian Pacific long distance passenger train that had slowed after reaching a failed signal. Seven people were killed in the accident. The second case study focuses on the Southall rail crash [2]. A First Great Western InterCity passenger train from Swansea to London Paddington, operating with a defective Automatic Warning System (AWS), went through a red signal and collided with a freight train leaving its depot. The train was also fitted with an Automated Train Protection (ATP) system but this was switched off. Six people were killed and over 150 were injured.

The third case study focuses on the Überlingen accident. This 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 final case study focuses on the accident at Milan's Linate airport on the 8th October 2001 [3]. An 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.

3. Management Priorities and Degraded Modes

Organisations often place undue emphasis on operational priorities that persuade staff to continue service provision even when safety is jeopardised. For example, the Glenbrook accident report makes many references to a 'culture of on-time running' that existed at the State Rail Authority of New South Wales [2]. The concern to meet the timetable deadlines led drivers to operate trains without functioning radios or with defective brakes; "degraded modes of operation accidents are more likely to occur, particularly if employees acting under the imperative of on time running are trying to have the infrastructure perform more efficiently than it is capable of doing" [2, p.150].

Operational priorities and organisational structure determined by management may also undermine co-ordination between different groups. It can be difficult for operational staff and maintenance teams to accurately convey their tasks and priorities to co-workers who have little experience or understanding of their different activities. For example, the Überlingen report described how the controller on duty 'had not been informed' about the presence of an additional manager intended to be the '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].

At Linate, there was a similar breakdown in information sharing 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 and comprehension between maintenance management and teams of operational staff who must continue to maintain levels of safe service in the face of latent failures.

4. Training, Safety Culture and Degraded Modes

The Glenbrook investigation team argued that "Many accidents occur during what is described as a degraded mode of operation…[because] the risk of accidents is increased if the procedures or training are inadequate or if there is a lack of an appropriate safety culture" [2, p. 43]. In particular, the driver of the inter-urban train "did not appear to have proper training in the operation and effect of Safeworking unit 245". Safeworking Unit 245 specified that extreme caution should have been used after passing an automatic signal at stop. The implication being that such caution would have enabled the inter-urban train to stop before colliding with the rear units of the Indian Pacific train. However, the particular actions of the train crews are often caused by underlying or latent problems in the safety management systems. These latent problems contribute to the context in which accidents occur under degraded modes of operation. ***Problems in training did not create the degraded modes of operation. However, lack of appropriate knowledge and skills may have undermined the engineers' or drivers' attempts to cope with the failures that were associated with these degraded modes***:

The argument that inadequate training left staff vulnerable to the problems created by degraded modes is repeated in the Southall accident report. A technical failure in the Automatic Warning System (AWS) left the driver of the passenger train without an important reminder of the aspect of the signaling system. At the time of the accident, there was some debate within the industry about the status of AWS. Many felt that it provided additional reminders to the driver and so should be viewed as a driver aid and not an essential safety-related system. In consequence, the driver had never driven a high speed train without AWS nor had he received any training on what to do without such support. Similar comments can be made about the lack of training that was cited as a reason why the driver was prepared to operate the train without operating the Automatic Train Protection (ATP) system that was installed on the unit. At the time of the accident, ATP training was not part of the operating company's system for Driver Competence Assessment. There was no company policy to match ATP competent drivers with ATP designated services [3, p. 55].

The ANSV and BFU investigations into Linate and Überlingen illustrated the importance of training in safety management. For example, the Air Navigation Service Provider involved in the Überlingen mid-air collision had recently established a Centre of Competence to develop expertise in areas such as risk assessment and safety monitoring functions. 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]. As a result there was a delay while these skills were built up. The lack of trained and experienced safety managers 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. 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].

Problems of competency and inadequate staffing levels undermine ATCO performance during degraded modes of operation. The use of Single Manned Operation Procedures (SMOP) in the Zurich ACC at the time of the Überlingen mid-air collision was an unofficial practice. , The BFU report acknowledges that "this way of proceeding … 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… Even though it was an unofficial procedure it was known to and tolerated by the management" [2, p.75]. The ATCO was alone as the second ATCO was out of earshot resting in the lounge. The remaining ATCO had to simultaneously perform the tasks normally associated with the Radar Planner (RP) and Radar Executive (RE) as well as the Chief Controller [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 particular number of operators is operating in a 'degraded mode' if there are less members of staff. In ACC Zurich, the Controller had 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 [2, pp.41-42]. The demands of these various tasks and the consequent disruption caused by moving between the different positions appears to have played a significant part in undermining his situation awareness.

5. Operating Rules and Degraded Modes

Regulators and operating companies recognise the safety implications of 'degraded modes' and, typically, respond by drafting rules to guide operator intervention. However, it can be difficult to identify all the problems that might restrict normal operations. This is illustrated by the regulations governing maintenance on the Automatic Warning System (AWS) prior to the Southall collision. In 1980, British Rail issued MTf169 which stated that a number of tests should be performed before any train is returned to service after a fault had been reported. Subsequently TEEICM/89/M/200 created potential confusion by specifying a number of additional checks. There were plans to incorporate these two documents but this never took place [3, p.67]. The rules governing degraded modes in terms of train operation with a failed AWS were also ambiguous. The drivers' Rule Book stated; **"**If it is necessary to isolate the AWS the driver must inform the signalman at the first convenient

opportunity. The train must be taken out of service at the first suitable location without causing delay or cancellation". It is unclear whether the train should be kept in service if delay or cancellation would otherwise be caused given that some interruption to normal service would occur unless a replacement train was immediately available.

The rules governing degraded modes of operation also played a significant role in the Glenbrook accident. A power supply unit that provided electricity to a train sensing circuit within the automated signaling system failed. The circuit overlapped two blocks of track and so caused two consecutive signals to 'fail safe' with a stop or red aspect. As required by Safeworking Unit 245, mentioned in previous sections, the driver of the Indian Pacific train obtained permission to proceed onto the next signal after the initial stop indication. The driver was concerned by the second red signal and so got out to use the signal post telephone. Again in accordance with the safeworking unit, he wanted to obtain further permission from the signaler to continue beyond the second signal. However, he failed to contact the signaler erroneously believing that the phone would not work because the 'press to ring button' was broken. He returned to the locomotive and following the provisions of 245 waited for a further minute to enable any trains ahead of his unit to clear the next section of track. The additional delay reduced the headway between the stationary Indian Pacific unit and the following inter urban train. The signaler told the driver of the inter urban train that he could "just trip past it". However, he continued to obey regulation 245 and requested permission from the signaller to pass; "I'm right to go past it am I mate?" elicited the response "Yeah, mate, you certainly are". The official report argued that the colloquial nature of this exchange gave the inter-urban driver the false impression that the track ahead was clear. The driver proceeded beyond the signal and was traveling at approximately 50km per hour when he saw the rear of the Indian Pacific train but was unable to avert the collision [2, p. 10].

Regulations have become so complex that many 'front line' staff only have a minimal grasp of the procedures that they are required to follow. One driver voiced the following criticisms of Safeworking Units; "My view is that they have become largely irrelevant to the guy that is doing…the job because they are more of a library addition, rather than an actual workbook I can take with me. It is pretty hard to carry all those manuals on the job with you" [2, p.130]. In the aftermath of both accidents, calls were made to improve drivers' understanding of the regulations that govern their interaction with degraded modes on their rail systems. Often these calls were made in spite of the observation that the rules and procedures were themselves flawed and would not have avoided the adverse outcomes.

A variety of different procedural violations were identified after the Linate runway incursion. The ANSV 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.

6. Incident Reporting

Incident reporting systems help to ensure the detection of, and response to, degraded modes of operations. Drivers and engineers can exploit fault tracking systems to alert maintenance crews and management staff to problems. However, management actions can undermine the 'reporting culture'. For example, the Glenbrook investigation revealed how a driver reported a defective signal that could not be replicated by a signal electrician. The driver was then charged with making a mischievous report. In another example, a driver/engineer was forced to continue operating a train even though he had filed a report to indicate that it had faulty brakes [2, p.45-6].

The structure and organization of the railway industry can complicate the reporting of faults. The Southall accident occurred in the aftermath of rail privatization in the United Kingdom. One consequence of this was that drivers were employed by different organizations, the train operating companies, from the signalers who were employed by the infrastructure providers, Railtrack. If the driver informed the signaler of a potential problem, the signaler would pass the information via their reporting structures to Railrack Control whereas the driver would report to the Train Operating Company's Control center. Although their different control centers were in close contact, the different reporting structures created confusion and made it difficult to trace faults that affected several different areas of the rail infrastructure [3, p.145].

Two previous air proximity violations had occurred and been investigated at ACC Zurich during the Single Manned Operation Procedures (SMOP) that were in force at the time of the accident.

These incidents had already led the Swiss BFU and BAZL to raise questions about SMOPs [2]. No formal review was used to assess the practice though it appears that the ANSP felt that SMOP was an unacceptable operating mode in the long term.

The ANSV also identified 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.

7. Human Factors and Operator Performance

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].

Increasing levels of workload also affected the ATCO prior to the Überlingen accident. 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.

The interface with automated systems plays an increasingly important role in the human factors issues that arise during degraded modes of operation. The Southall rail accident provides numerous insights into the temptation to maintain levels of service in the presence of automated systems failure. Before this accident, no risk assessment had been conducted for continuing operations without AWS. Had such an assessment been conducted then it might also have revealed the limitations of the AWS human machine interface. For example, the majority of signals passed at danger (SPADs) continue to occur with trains that are equipped with AWS; drivers cancel the warning and proceed without applying the brakes [3, p.141].

Different problems affected the implementation of Automated Train Protection (ATP) systems prior to the Southall rail accident. Initial trials of the ATP systems on the section of track involved in the Southall collision suffered from problems of water ingress and from vibration failures. A revised system suffered from software problems; it identified potential collisions with following trains when the system underestimated the distance that the lead train had traveled. Drivers were faced with a number of spurious emergency brake applications. Following the Glenbrook accident, it was revealed that ATP equipment was the greatest single item of maintenance on the Queensland system. Two subsequent train collisions in 1989 and 1994, stemmed in part from the installation of ATP; 'the first collision was brought about by the driver having insufficient air left within the braking system to apply the brakes on the train as the Swedish system had been bought off the shelf and had never been designed to cope with the problem of low air… the second accident in 1994 occurred because the driver kept overriding the system' [2, p.154].

The media and the general public have urged the installation of ATP as a means of guarding against driver errors of the kind witnessed in the Southall accident [2, 3, 4]. However, such public pressure has often overlooked the maintenance and reliability problems. This is important because, as we have seen with AWS, there are significant consequences if operational staff become used to 'working-around' failed systems that might otherwise play a significant role in supporting their everyday tasks. The official investigation into the Glenbrook collision makes this point; 'Each time you have a failed ATP system, you are back into degraded mode, where you have to depend on the human behavior, and as we have seen so often, the real problem is not so much equipment issues, but what happens when that equipment fails' [2, p.155].

8. Degraded Modes and Risk Management

Abnormal or increased loadings can be tolerated for short periods providing that the potential hazards have been identified and

appropriate mitigations have been introduced. Risk assessments can be used to support this form of hazard analysis under degraded modes of operation. It can, therefore, be argued that the four accidents were the result of inadequate risk assessments. Degraded modes eroded the safety margins that usually protected normal operating practices. For example, the Glenbrook report argued that a Rail Safety Inspectorate should be introduced to ensure that all of the parties involved in running the railways cooperated in their hazard assessments and in their risk mitigation strategies. The justification for the creation of such a body was based on the observation that many organisations seem to be 'struggling' with the prerequisites for safe operations. Some groups used Australian Standard 4292 to guide their risk management while others adopted a combination of this standard and 4360. In some cases, the decision to use both 4292 and 4360 'produced little more than a bureaucratic structure' [2, p.169]. These structures were said to have achieved little in terms of safety outcomes for both staff and the general public. Similarly, the Überlingen report noted that the supervisor who was responsible for briefing the ATCOs did not identify the specific hazards related to the maintenance work that had been scheduled. He considered that the Systems manager was responsible for this; 'he did not recognise the safety issue and did not suggest appropriate measures to mitigate the risk, e.g., [that] both ATCOs remain on duty while the technical work was in progress' [4, p.87].

The Southall accident report criticizes a number of risk assessments. For example, changes in the staffing at the Old Oak Common Maintenance Depot reduced levels of support for the engineers trying to trace the cause of the reported AWS failure. These changes in demarcation were subject to internal and external risk assessments. However, neither identified the potential stresses that were placed on shift supervisors who struggled to oversee these maintenance tasks [3, p.64]. Similarly, the train operator commissioned a risk assessment before privatization to consider the potential impact of single driver operations. The report was centered on a risk matrix and concluded that for speeds above 110 miles per hour, a second driver marginally *increased* the risk with or without ATP [3, p.59]. However, this report did not consider the risks of single driver operations for High Speed Trains without either AWT or ATP. The Southall accident report concluded that 'the situation has been reached where any change not accompanied by risk assessment is greeted with surprise, if not disbelief' [3, p.194]. There are no guarantees that such techniques will anticipate all of the potential hazards that can arise during the operation of safety critical systems. This can, in turn, create overly optimistic results from quantitative assessments.

9. Conclusions

Degraded modes of operation occur when technological systems fail to meet the levels of service that are expected by staff and managers. Over time, operators develop 'work arounds' that help them to cope with these degraded modes. This has led to a culture of 'making do' where co-workers try their best to maintain service provision in spite of system failures. These adaptations and 'work arounds' undermine safety. This paper has presented some of the reasons why teams of co-workers continue to operate safety critical systems when key elements of their infrastructure have been compromised, for example during routine maintenance. These include management pressures to sustain levels of service and the difficulty of reporting faults that often affect both operating companies and infrastructure providers.

Four accidents in the rail and air traffic management industries have been used to illustrate the analysis. The Überlingen mid-air collision took place when ATCOs struggled to maintain service provision while changes were made to their Local Area Networks. The Linate runway incursion occurred when the lighting, radar and signage had gradually degraded over a prolonged period of time. The Glenbrook rail collision occurred when a driver failed to make contact with a signaller because he thought the track-side phone was inoperative. Finally, the Southall collision occurred when the driver of a High Speed Train was left to operate a train without the support of either AWT or ATP. The similarities between these accidents suggest that the problems of degraded modes of operation will not disappear in the near future. We must continue to improve our understanding of the reasons why operators try to maintain service while system failures undermine application safety.

References

1. Railway Group Standards, Section 6, Railway Safety: Operations, February 2007.

2. Inquiry into the Glenbrook Rail Accident-Final Report, Chaired by P. A. McInerney, New South Wales Independent Transport Safety and Reliability Regulator, Sydney, Australia, April 2001.

3. Southall Rail Accident Inquiry Report, J. Uff, UK Health and Safety Executive Books, London, 2000. ISBN 0 7176 1757 2

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.

5. L. Bainbridge, Ironies of Automation. In J. Rasmussen, K. Duncan and J. Leplat, (eds.) *New Technology and Human Error*, Wiley, Chichester, pp. 276-283, 1987.