Scaring Engineers with Degraded Modes: The Strengths and Weakness of Action Research in Air Traffic Management

Chris W. Johnson and Andrew Kilner*

Department of Computing Science, University of Glasgow, GL2 8RZ,
Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

*Safety R&D, EUROCONTROL Experimental Centre, Bretigny-sur-Orge, F91222, France,
Andrew.kilner@eurocontrol.int

Abstract

Degraded modes of operation occur when operations and engineering teams work to maintain levels of service even though critical elements of their underlying technical infrastructure have failed. In most situations, these 'work arounds' and ad hoc fixes do not threaten safety. However, the Linate runway incursion and the □berlingen mid-air collision have shown that degraded modes of operation combine with human error and other forms of system failure to create preconditions for major accidents. This paper describes initiatives to exchange lessons learned about engineering failures between European Civil Aviation Conference (ECAC) states. The approach has been guided by an 'action research' methodology in which a series of site visits and observational exercises informed the development of awareness raising materials. The close involvement of stakeholders was informed by findings from previous research initiatives into the operational impact of safety culture within air traffic management organisations. This action research approach provided significant benefits. In particular, we obtained immediate positive feedback in support of rapid risk assessment techniques. However, the action research focus on close consultation with stakeholders also raised a host of longer term questions, for example about the relationship between these lightweight hazard analysis methods and more established approaches in safety management. These remain to be addressed by more traditional research methodologies.

Keywords: Degraded Modes of Operation, Action research, ATM Safety.

1. Introduction

Degraded modes of operation occur when teams work to maintain levels of service even though critical elements of their technical infrastructure have failed. They pose a significant concern for the future of Air Traffic Management because we cannot guarantee the reliability of increasingly complex, interactive, software-intensive systems. Degraded modes of operation characterise everyday experience; engineers and operational staff routinely find ways to cope with a myriad of low consequence failures. However, previous accidents at Linate and □berlingen show that minor problems quickly combine to create the preconditions for major failures (Johnson, 2006).

This paper describes the research and development practices that informed an awareness raising initiative across ECAC states. An action research methodology was used to ensure a tight integration between stakeholder requirements and previous research into the impact of safety culture on ATM operations. This was used to inform the creation of 'awareness raising' materials. The aim was to transfer 'lessons learned' in combating the hazards created by degraded modes of operation. An initial series of site visits helped to establish detailed stakeholder requirements from ANSPs, regulators and equipment manufacturers. This involved interviews, discussions with senior management and observational studies with engineering teams. From this, we focussed on a series of workshops to communicate the safety implications of Degraded Modes on ATM safety. This represented a considerable change of emphasis. Previous initiatives had focused on operational and management staff rather than systems engineering teams. Other innovative features focused on the development of rapid risk assessment techniques. These are intended to help service providers identify the hazards of system failure during everyday operation. Conventional risk assessments are, typically, only conducted during major system upgrades or the procurement of new applications. In contrast, our approaches were intended to be lightweight and flexible so that they could be applied at minimal costs to inform everyday engineering decisions.

Over a twelve month period, a series of novel techniques were developed to synthesise theoretical material on risk assessment and 'real world' scenarios of degraded modes provided by ANSPs and manufacturers from across Europe. The intention was to provide general insights into the nature of the problem in a form that was relevant to working engineers. Pilot studies were then conducted with the systems teams in three ECAC service providers. Subsequent sections of this paper present the feedback that was obtained from these initiatives – both in terms of the insights they provided about degraded modes of operation and the utility of action research as a methodology for safety innovation in air traffic management.

The first trial involved one of Europe's larger ANSPs. Many of the engineers had a good knowledge of risk assessment and safety management techniques. Before the course, there was a general belief that established risk assessment process addressed most of the hazards associated with degraded modes of operation. However, it transpired that many risk assessments were not conducted at the times when hazards were manifest, nor did the risk assessment process link to operations and the impact on operations. The second trial involved engineering teams from a smaller ANSP. Many of the participants involved in the study were largely unaware of the concept of degraded modes of operation. They had limited experience of risk assessment. In this case, additional emphasis had to be placed on explaining the principles and vocabulary of safety management, enshrined in the SES regulations. The final ECAC state helped to illustrate the diversity of expertise within the same service provider. Many engineers had a strong background in risk assessment and had already developed techniques for dealing with the hazards created by degraded modes of operation. Others had no exposure to these ideas even though they recognised the symptoms of infrastructure failure from their everyday work experiences.

2. Methodological Background: Action Research

The work in this paper was guided by the application of action research within air traffic management. Informally, this iterative approach begins by working with a group of stakeholders to identify a shared set of problems. It continues by identifying potential solutions. The same cooperative approach is then used to implement and evaluate potential countermeasures. At first glance, action research might seem to share much in common with standard professional practice or with the cooperative problem solving techniques used by many commercial consultancies. Differences stem from the emphasis that action research places on theoretical insights from science and engineering. This creates a two way process in which applied problem solving is both informed by and helps to inform existing research findings. Our work on degraded modes of interaction was guided by previous theoretical studies on the relationship between safety culture and safety management (Gordon and Kirwan, 2005, Pidgeon and O'Leary, 1994). At the same time, our studies have been forced to extend the previous research in this area by looking beyond the impact of safety culture on operational staff to consider the effects that safety culture can have upon the engineering of degraded modes of operation. This two-way process creates methodological problems. For example, there is no assumption that participants in action research will remain objective. The stakeholders work with the rest of the investigators both to identify relevant research from previous theoretical studies and also to establish an agenda for further study.

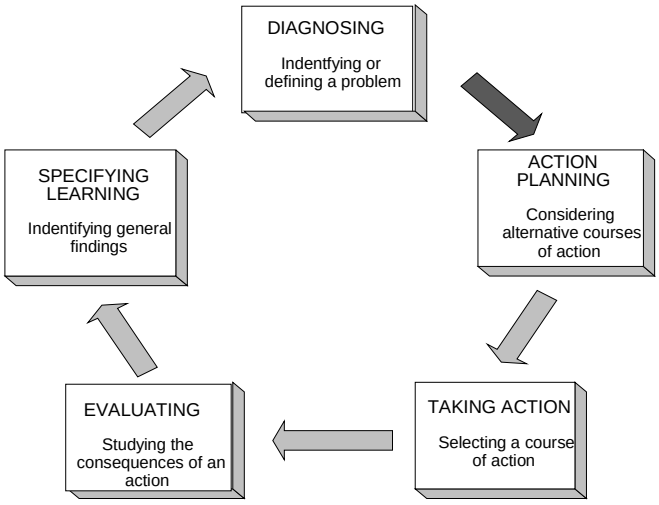


Figure 1: Susman's Action Research Framework

Figure 1 provides an overview of the stages that can be used to structure action research (Susman, 1983). Information is gathered about common problems; this process also helps to identify relevant previous research that guides subsequent diagnosis. The next step is to identify a number of potential countermeasures using the scientific and engineering literature to select an appropriate strategy. The utility of any subsequent intervention is then assessed; this phase may also help to identify requirements both for subsequent intervention and also for further research. The individual phases in Susman's model are used to structure the rest of this paper.

3. Diagnosing

The first stage of Susman's approach to action research focuses on the diagnosis of 'real world' problems and the identification of relevant research. Our concerns over the safety impact of degraded modes were triggered by research studies into the common causes of accidents involving Air Traffic Management. In particular, we identified that the loss of critical infrastructures had contributed both to the Überlingen and Linate accidents (Johnson, Kirwan and Licu, 2009). At Überlingen, there was no sustained hazard assessment prior to a major system upgrade in the sectorisation associated with Revised Vertical Separation Minima (RVSM). Partly in consequence, the systems and operations teams failed to anticipate demands that were placed on a single ATCO as he struggled to respond to the degraded modes that resulted from the loss of key communications, short-term conflict warnings and radar planning applications. At Linate, there was a longer-term degradation in the supporting infrastructures. Technical problems and complex managerial structures led to significant delays in replacing analogue ground movement radar systems and runway lighting. Ground signage was not maintained to an adequate level. Although these accidents occurred in 2001 and 2002 the legal proceedings have continued. On April 16, 2004, a Milan court sentenced the airport director and an air-traffic controller to eight years in prison (Johnson, 2006). The former head of the air traffic controllers' agency and the former head of the airport were given six and a half years. Meanwhile, the Swiss courts handed down suspended prison terms to three of the Skyguide managers involved in the Überlingen accident.

One of the key differences between action research and more general consultancy or participatory design is the closer integration of engineering and scientific studies into the analysis of existing problems. The early stages of our work on degraded modes of operation were strongly influenced by previous work on the impact of safety culture on ATM operations. This related to key findings in the BFU Überlingen report "The Company was in the process of evolving a functioning safety culture which they could not, however, fully realize at that time" (BFU 2004, page 93). Similarly, the ANSV report into the Linate runway incursion argued that "The absence of a specific culture and of a functioning Safety Management System, has limited each actor at the aerodrome to see the overall picture regarding safety matters" (ANSV, 2004, p. 117). Both reports draw strong links between safety culture within complex organizations and the attitudes of staff and management to degraded modes of operation. Previous research in this area by Reason (1997) and Pigeon and O'Leary (1994) has identified four principal components of safety culture:

1. A reporting culture encourages employees to divulge information about all safety hazards that they encounter.
2. A just culture holds employees accountable for deliberate violations of the rules but encourages and rewards them for providing essential safety-related information.
3. A flexible culture adapts effectively to changing demands and allows quicker, smoother reactions to off-nominal events.
4. A learning culture is willing to change based on safety indicators and hazards uncovered through assessments, data, and incidents.

Several organizations have translated these high-level objectives into tools and techniques that are used to promote the development of appropriate safety cultures within their industries. For instance, Figure 2 illustrates the high-level components of safety-culture within Air Traffic Management. The four elements of Reason's model (reporting, just, flexible and learning cultures) refer to general attributes of safety culture. In contrast, the three elements of our model focus more directly on attitudes and beliefs. They are, therefore, complementary views.

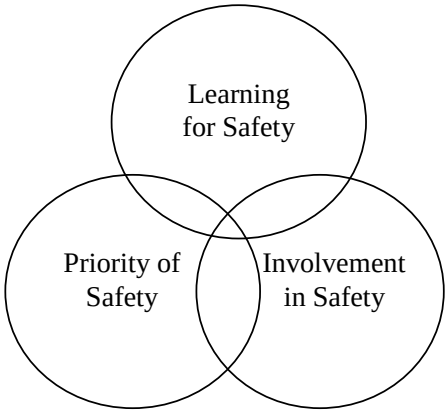


Figure 2: Components of Safety Culture

As mentioned in Section 2, the action research methodology cannot simply rely on previous academic research or even on an abstract analysis of accident reports. It must also build upon close engagement with a range of stakeholders. Over the last two years, EUROCONTROL has used a number of questionnaires to help ANSPs assess their safety culture. These include questions about attitudes to safety:

- Is 'safety first', or 'capacity first' the working reality in your organization in its daily activities?
- How do you ensure that safety is not compromised by the drive for better productivity?
- Who decides the quantity and quality of safety assurance resources in your organization?

These surveys have been distributed to service providers from across Europe. However, the intention has not been to provide a superficial comparison across ECAC states. Instead, the developers have worked with each ANSP to tailor questions to the concerns and requirements of individual organizations. A series of de-briefing workshops have also been held help to assess the results and identify areas for further work within the service providers' organization (Gordon and Kirwan, 2005). These safety culture surveys did not initially include questions about the engineering or operational impact of degraded modes. An additional set of questions was therefore included to assess the interaction between safety culture and systems engineering.

4. Action Planning

Our previous work on the causes of Linate and □berlingen combined with the insights provided from the safety culture surveys to suggest that there was an urgent need to gather more detailed information about how different European ANSPs addressed the problems created by degraded modes of operation. The questionnaires suggested that many service providers had strong safety cultures within their engineering teams but that there were common concerns, for example that the sub-contractors who supported ATM infrastructure maintenance did not always operate to the same standards of safety management as direct employees. We, therefore, moved from an initial diagnosis about common problems in systems engineering to develop a more detailed plan of action to both validate the diagnosis and identify further scope for intervention.

A series of site visits were, therefore, organized with staff at all levels within Air Navigation Service Providers in different areas of Europe. The intention was to gather information on technical equipment and maintenance processes as well as staff attitudes to working with degraded mode of operations. Stakeholders included controllers, technical staff and operations supervisors as well as safety teams and senior management. These meetings extended across several days, consisting of interviews and focus groups during which extensive notes were taken. These were then transcribed so that participants could identify any inaccuracies within 24 hours of the meetings having taken place. Observational shadowing was also possible with individual Air Traffic teams and with groups of systems engineers. This was important because it was possible to see how different stakeholders interacted as they worked together to solve infrastructure failures during routine operations.

These elicitation exercises were conducted in areas of Europe with very different traffic patterns. Some visits looked at major ATM service providers that acted as hubs for numerous regional traffic flows. Other providers operated more limited national and regional services. Further consultations were held with representatives of the FAA and NAV Canada to obtain a wider perspective on the problems of degraded modes of operation and the maintenance of an appropriate safety culture. Subsequent interviews and focus groups were held with a number of ATM system suppliers and integrators. This provided important insights into the problems that can arise when ANSPs rely on engineers employed by other organizations to implement major changes in their underlying systems. The main focus of all this work was to identify 'lessons learned' rather than 'blame and shame' the stakeholders who were at the heart of this initiative.

Figure 3 shows how we used the theoretical model of Safety Culture illustrated in Figure 2 to provide an analytical framework for observations derived from the site visits (Johnson, Kirwan and Licu, 2009). This provides a further example of the tight integration between previous studies and interventions embedded within the principles of action research summarised by the Susman model. In this case, the three-part model provides a bridge between work on safety culture and degraded modes of operation. Different versions of the diagram shown in Figure 3 were created for ANSPs supporting various traffic patterns. Figure 3 looked at ANSPs with high volumes of traffic passing through their airspace but relatively limited amounts of domestic traffic. A second diagram was created for service providers characterized by high volumes of both domestic traffic and over-flights. A final grouping analysed ANSPs with large volumes of domestic, regional traffic but a smaller volume of international traffic.

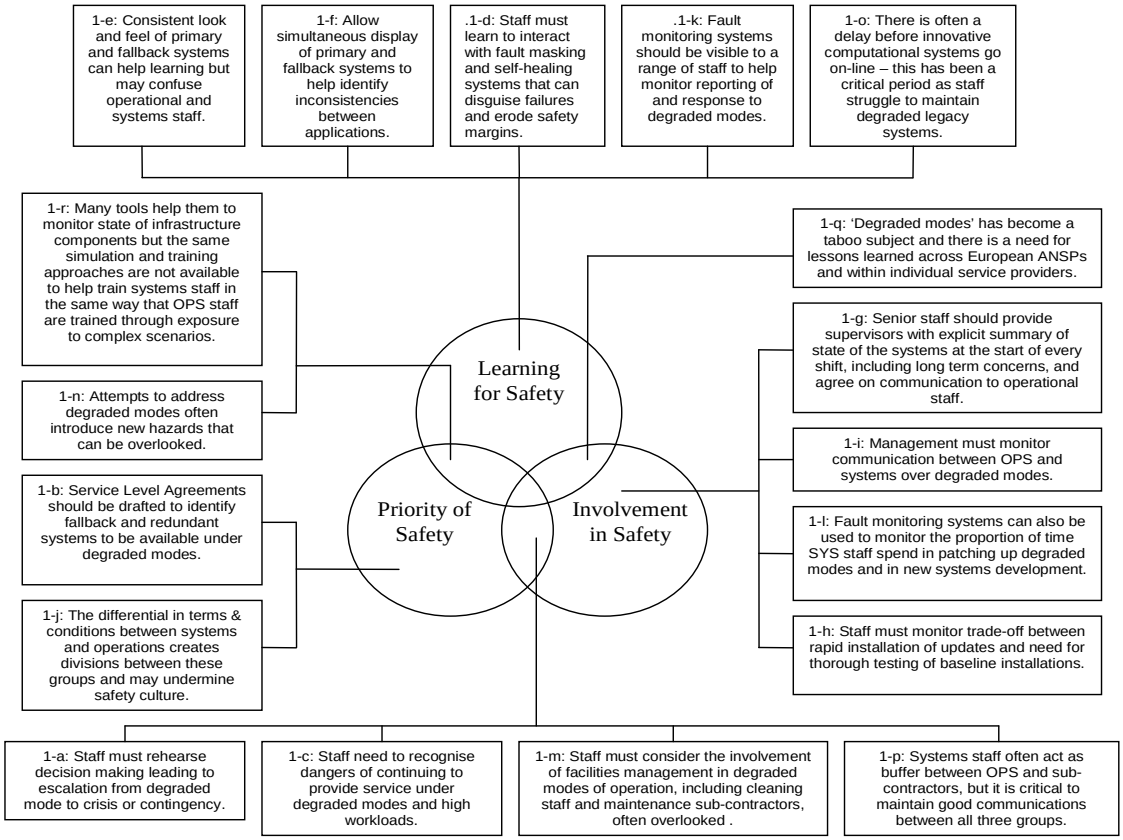


Figure 3: Overview of Safety Culture and Degraded Modes in the First Group of ANSPs

Figure 3 deals with the relationship between safety culture and degraded modes for ANSPs supporting high volumes of traffic passing through their airspace but relatively limited amounts of domestic traffic. During the sites visits, both operational and technical staff were keen to stress that redundant and fallback systems both support the overall reliability of safety-critical systems and increase the 'peace of mind' that is necessary to operate at high levels of workload. Several ATCOs described how capacity would be cut during degraded modes of operation if the fallback system was unavailable even though the primary application was unaffected because they had lost the additional assurance provided by 'defense in depth'. Peace of mind depends on both the availability of fallback systems and the

stability of main system infrastructures. In this view, fallback systems not only provide resilience against degraded modes of operation, they can also be seen as 'capacity enablers'. Problems arise under degraded modes of operation when staff can be pressured to sustain high levels of service without the assurance of redundant and fallback applications. Standard operating procedures and minimum equipment lists provide some protection against these problems. However, they may be ignored or suspended through the use of waivers. The staff in one of the ANSPs in this first group acknowledged that this was possible in their organisation. However, they also argued that the promotion of a strong safety culture helped to mitigate pressures to sustain high levels of service without key elements of the underlying infrastructure. These observations led to the introduction of the following observation into Figure 3:

Observation 1-c: Problems are likely to occur when high-levels of workload continue to be accepted without the reassurance provided by redundant and fallback systems. These applications make it possible to continue service provision *even when it may not be advisable* to sustain services at this level.

A further example of the concerns identified through this integration of scientific study and direct observations in action research can be provided by observation 1-d. One of the focus groups in this first group of ANSPs discussed a fault masking application. These systems support situation awareness by filtering the number of warnings that are normally presented to operators. In such circumstances, ATCOs may not be aware of the state of key components in their underlying infrastructure. This focus group also discussed future projects for 'self-healing' systems where fault tolerant computer architectures automatically transfer control to redundant applications without necessarily warning system operators. These applications offer considerable benefits in terms of maintaining levels of service in the presence of failure. However, there are considerable risks if systems staff fail to correct any faults that have been masked by the automatic use of redundant systems (Johnson and Holloway, 2007). This led to the introduction of a further observation into Figure 3:

Observation 1-d: Self-healing systems and fault masking applications can be dangerous if systems staff and operational teams are unaware that they are now operating without the protection of either redundant or fallback resources. Self-healing systems must ensure that necessary maintenance is conducted to restore primary applications.

The action research methodology not only promotes the close integration of academic and applied concerns. It also promotes appropriate interventions to address the stakeholder problems elicited during the initial phases of any study. In the context of our work, it was not sufficient simply to produce graphical maps of the interactions between degraded modes of operation and safety culture such as those illustrated in Figure 3. It was, therefore, necessary to take actions that might help to avoid any recurrence of the events leading to Linate or □berlingen. Fortunately, the overviews provided by our application of the 3-stage safety culture model provided a firm foundation upon which to build subsequent interventions.

5. Taking Action

Although the graphical overviews of the questionnaires, focus groups, site visits and workplace observations, illustrated in Figure 3, provided a starting point for our subsequent interventions, there was no automatic means of identifying what should be done. Instead, further meetings were organised with a range of stakeholders. The first issue was to determine the objectives for the intervention. These can be summarised by the following list:

- **Promoting discussion not 'rote learning'.** The action research perspective adopted in this work helped to emphasise the complexity of the problems that we were studying. For instance, some ANSPs responded to degraded modes of operation by creating a 'minimum equipment list' that specified basic infrastructure standards for service provision. However, this included equipment that was not available to neighbouring ANSPs. Others associated different levels of traffic that could be supported depending on the level of system support that was available. Most ECAC states had not formalised this relationship, instead relying on the experience and expertise of operational and engineering management. A further concern was that the earlier phases of the project could only provide limited insights into the detailed engineering and operational environment of each member state. The diversity of practice

combined with the complexity of local operations implied that any subsequent intervention should focus on discussion rather than the 'rote learning' of safety management principles that might be extremely difficult to apply within each particular ECAC state.

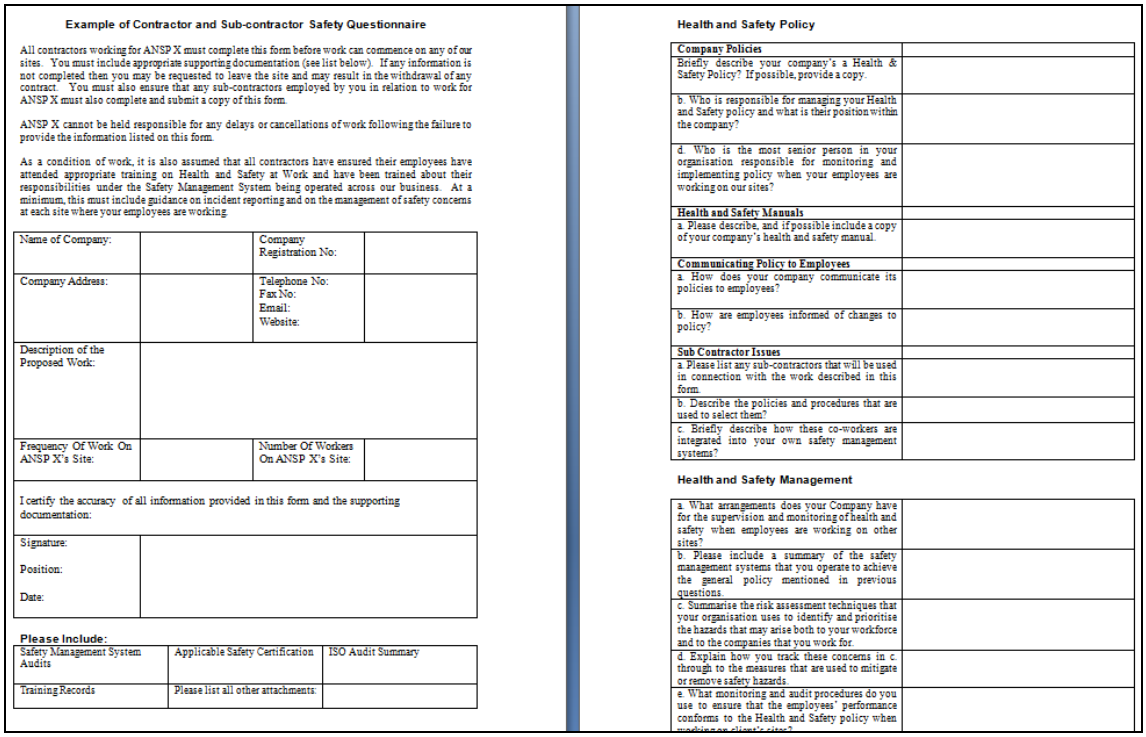
- **Focus on systems engineering not just operations.** Earlier sections of this paper have argued that the action research methodology cannot deliver the objectivity of more controlled forms of analysis. Many of the individuals involved in the elicitation phase of this work came from engineering, rather than an operational, background. It is therefore unsurprising to learn that the focus of the proposed interventions was on the systems engineering aspects of degraded modes of operation. The justification for this was a perceived imbalance between the previous focus of many previous courses and workshops on operational issues. A further motivation was that degraded modes of operation are often first identified by engineering teams. As we shall see, subsequent analysis has questions some aspects of this initial decision – perhaps reflecting a weakness inherited from the action research methodology.

- **Awareness Raising through Case Studies and Lessons Learned.** One concern expressed by stakeholders was that many ANSPs were 'in denial' over systems engineering problems. Too often, it was argued that degraded odes did not have any significant impact upon operational safety. However, others in the same organisation often expressed great concern over the impact of system failures. These individuals often provided specific case studies of incidents that had occurred in their organisation. These were used to provide a series of anonymised case studies with permission from the ANSPs. The intention was to ensure that awareness raising material and subsequent group discussions were based on previous accident reports, including those following Linate and □berlingen, as well as 'real world' case studies.

- **Focus on 'light weight' rapid risk assessment.** The final objective for intervention was to identify risk assessment techniques that could be delivered to a range of engineering teams without the costs, in terms of training and time, which are associated with many existing approaches. There was a concern that many of the methods advocated by regulatory or supervisory authorities were too complex to be used to during many of the more routine operations that had led to degraded modes of operation. This decision triggered a further iteration of the action research loop illustrated in Figure 1. Additional stakeholder meetings and electronic discussions were launched with engineering management from across Europe to gather a range of 'rapid risk assessment' techniques that might be promoted within any subsequent interventions. These ideas were supplemented by input from a range of other industries and organisations including the US Army and the International Atomic Energy Agency, which had already pioneered low cost risk assessment techniques to address the problems associated with degraded modes of operations.

The identification of these objectives led to the development of a two-day workshop format. The first day focused on an introduction to the detailed engineering causes of the Linate and □berlingen accidents, as documented by the ANSV and BFU. These were supplemented with less detailed presentations about 7 further incidents contributed by ANSPs during previous phases of the project. These ranged from the loss of an ACC following the failure of a UPS through to ground collisions caused by issues in the maintenance of ground movement radar systems. The second day built on these previous incidents to consider potential solutions based on rapid risk assessment. Again case studies were used – including the software related failure of an ATM local area network through to the devastating impact of a more 'mundane' fire in a machine room.

A series of forms and procedures were incorporated into the material that was to be delivered. The intention was to provide specific examples of the 'good practices' identified in visits to ECAC states. For example one of these documents was contributed by an ANSP to help other service providers assess the safety management processes used by the companies that sub-contract systems engineering services. This document is illustrated in Figure 4. As can be seen, it asks questions about the safety management systems within an external supplier. The aim behind this form is to help identify whether there are any additional hazards that might be associated with the use of a sub-contractor that might not arise from directly employed staff. This is increasingly important given that few ANSPs will have the broad range of computational and advanced engineering skills that may be required to implement many of the innovative architectures being proposed across the SESAR programme.



Example of Contractor and Sub-contractor Safety Questionnaire

All contractors working for ANSP X must complete this form before work can commence on any of our sites. You must include appropriate supporting documentation (see list below). If any information is not completed then you may be requested to leave the site and may result in the withdrawal of any contract. You must also ensure that any sub-contractors employed by you in relation to work for ANSP X must also complete and submit a copy of this form.

ANSP X cannot be held responsible for any delays or cancellations of work following the failure to provide the information listed on this form.

As a condition of work, it is also assumed that all contractors have ensured their employees have attended appropriate training on Health and Safety at Work and have been trained about their responsibilities under the Safety Management System being operated across our business. At a minimum, this must include guidance on incident reporting and on the management of safety concerns at each site where your employees are working.

Name of Company:		Company Registration No:	
Company Address:		Telephone No: Fax No: Email: Website:	
Description of the Proposed Work:			
Frequency Of Work On ANSP X's Site:		Number Of Workers On ANSP X's Site:	
I certify the accuracy of all information provided in this form and the supporting documentation:			
Signature: Position: Date:			

Please Include:

Safety Management System Audits	Applicable Safety Certification	ISO Audit Summary
Training Records	Please list all other attachments:	

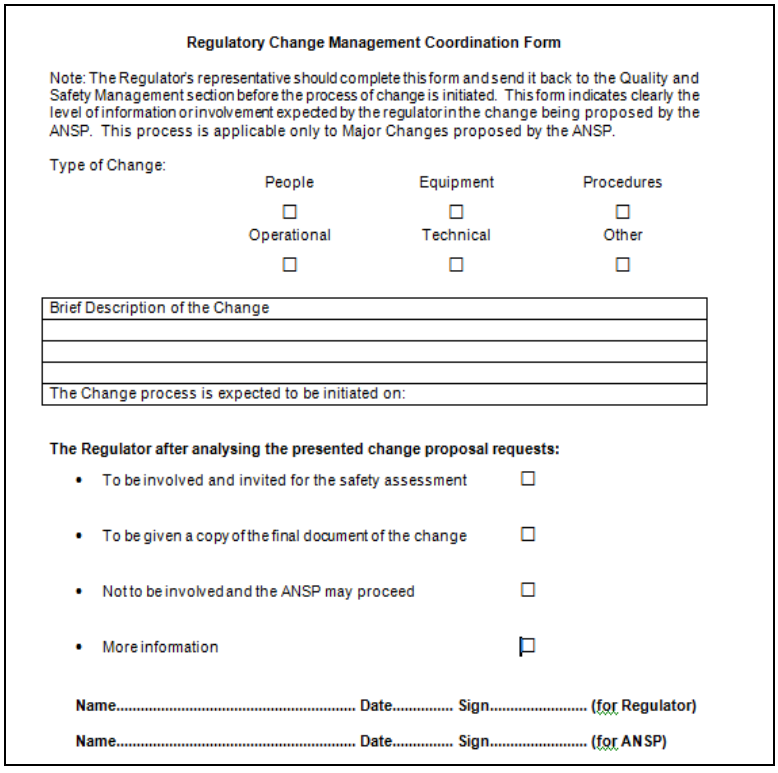
Health and Safety Policy

Company Policies	
Briefly describe your company's a Health & Safety Policy? If possible, provide a copy.	
b. Who is responsible for managing your Health and Safety policy and what is their position within the company?	
d. Who is the most senior person in your organisation responsible for monitoring and implementing policy when your employees are working on our sites?	
Health and Safety Manuals	
a. Please describe, and if possible include a copy of your company's health and safety manual.	
Communicating Policy to Employees	
a. How does your company communicate its policies to employees?	
b. How are employees informed of changes to policy?	
Sub Contractor Issues	
a. Please list any sub-contractors that will be used in connection with the work described in this form.	
b. Describe the policies and procedures that are used to select them?	
c. Briefly describe how these co-workers are integrated into your own safety management systems?	

Health and Safety Management

a. What arrangements does your Company have for the supervision and monitoring of health and safety when employees are working on other sites?	
b. Please include a summary of the safety management systems that you operate to achieve the general policy mentioned in previous questions.	
c. Summarise the risk assessment techniques that your organisation uses to identify and prioritise the hazards that may arise both to your workforce and to the companies that you work for.	
d. Explain how you track these concerns in c. through to the measures that are used to mitigate or remove safety hazards.	
e. What monitoring and audit procedures do you use to ensure that the employees' performance conforms to the Health and Safety policy when working on client's sites?	

Figure 4: Rapid Risk Assessment Forms for Sub-Contractor Services



Regulatory Change Management Coordination Form

Note: The Regulator's representative should complete this form and send it back to the Quality and Safety Management section before the process of change is initiated. This form indicates clearly the level of information or involvement expected by the regulator in the change being proposed by the ANSP. This process is applicable only to Major Changes proposed by the ANSP.

Type of Change:

People	Equipment	Procedures
☐	☐	☐
Operational	**Technical**	**Other**
☐	☐	☐

Brief Description of the Change
The Change process is expected to be initiated on:

The Regulator after analysing the presented change proposal requests:

- To be involved and invited for the safety assessment ☐
- To be given a copy of the final document of the change ☐
- Not to be involved and the ANSP may proceed ☐
- More information ☐

Name..... **Date**..... **Sign**..... **(for Regulator)**

Name..... **Date**..... **Sign**..... **(for ANSP)**

Figure 5: Rapid Risk Assessment Forms for Regulatory Change Management

Another document was intended to help regulators use ANSPs' risk assessments to determine whether or not they wanted to be consulted during subsequent phases of a systems engineering project. This resource was contributed by a service provider with a relatively small safety team. They were concerned that considerable time and energy was wasted in bringing a regulator 'up to speed' when had not been involved in the previous stages of a project. Figure 5 illustrates the simple format that was used to document the regulators decision about the degree of involvement they anticipated within a

system change. Key attributes of the form are that the change has to be described in a concise manner – too often regulatory resources are wasted by notifying them of changes in long and protracted documents that cannot easily be summarised. In such situations, regulators often revise their initial decision not to be involved in an earlier stage of development when they eventually realise the full extent of a proposed development.

6. Evaluating

Before delivering the first of these 'awareness raising' events, a pilot run was tested with the project team and other individuals within the EUROCONTROL research community. Significant revisions were made – these reinforced many of the key concepts within action based research. Participants argued that the focus on case study material and on the rapid risk assessment materials derived from the stakeholder visits obscured some of the underlying theoretical insights. Hence a stronger relationship was forged with previous research work. At the same time, it was also felt that the programme was too passive – participants did not get enough opportunity to engage actively with the material. In consequence, additional activities were introduced where, for instance, participants were asked to develop ATM versions of the credit card mnemonics that the US Army had developed to promote low-cost, rapid risk assessment techniques, illustrated in Figure 6.

Figure 6: Rapid Risk Assessment Mnemonics (Ack: Fort Rucker, US Army)

We were careful not to publicise the meetings as 'training' – the intention was to increase awareness about the significance of safety culture for engineering through considering the hazards from degraded modes of operation. The initial 'awareness raising' events were held with two service providers in very different regions of Europe. The first ANSP was in a relatively new member state, although they supported a diverse and growing mix of traffic. Their engineering teams had operated under very different political regimes and significant recent investments had brought in both new staff and new infrastructures. Many of the participants involved in the study were largely unaware of the concept of degraded modes of operation. They had limited experience of risk assessment. In this case, additional emphasis had to be placed on explaining the principles and vocabulary of safety management, enshrined in the SES regulations.

The second trial involved one of Europe's larger ANSPs. Many of the engineers had a good knowledge of risk assessment and safety management techniques. Before the course, there was a general belief that established risk assessment process addressed most of the hazards associated with degraded modes of operation. However, it transpired that many risk assessments were not conducted

at the times when hazards were manifest, nor did the risk assessment process link to operations and the impact on operations.

The third trial expanded the scope of the initiative. In this case, the safety management within the ANSP requested that the course be delivered several times to engineers in different areas of the country. This raised new challenges as it became apparent that the previous expertise and exposure both to the concepts of risk assessment and the hazards from degraded modes of operation was very different even within the same organisation. Some staff with many years in systems engineering were familiar with the language of risk assessment and had many examples of the hazards that arise from infrastructure failures. In contrast, many new recruits had yet to participate in training about risk management and had not met the key concepts within their University or vocational education.

7. Specifying Learning

Action research relies upon a formal process of evaluation to determine how well any intervention meets the needs of the stakeholder groups. In the context of this course, it was difficult to determine appropriate metrics with which to assess the impact of the two day sessions. Test-retest protocols simply demonstrate short term changes in expressed opinions. We were acutely aware that previous studies of safety culture had stressed the different between 'what we say' and 'what we think' and 'what we do'. Hence, the states chosen in this initial group were selected because they are participating in the on-going projects looking at wider forms of safety-culture measurement. Hence, we can use subsequent results from the surveys mentioned in previous sections to determine whether or not the pilot studies and initial presentations have had any longer-term impact. However, these studies take many months to administer and in the meantime we required more immediate feedback to improve the quality of subsequent events. It is for this reason that each delivery of the awareness raising material was followed by a formal 'de-briefing' session where an external observer asked each participant to contribute both positive and negative observations about the event.

The evaluations that were conducted after the awareness raising events led to a number of changes being made to the format and content of the material that was presented about the degrade modes case studies and about the rapid risk assessment materials. The can be summarised by the following list:

- ***'Don't scare us'.*** In many respects the case study material that was presented over the two days was too effective. Many of the workshop participants were surprised at the range of different hazards that were identified in the course. One particularly effective case study described how a faulty Uninterruptible Power Supply led to the closure of an ACC. Another described how engineers lives were placed at risk during a fire by a security door in the machine room that failed closed. These, typically, generated sustained discussion about whether similar failures were possible within each of the sites that we visited. The evaluations did not recommend major changes to this material but instead suggested that more of the rapid risk assessment material should be included to provide more of a positive message about how to avoid some of the failures that had been described during the site visits with engineering teams.

- ***'Less material about the Army Experience'.*** We had followed the action research approach outlines in previous sections. One aspect of this was to build upon previous research into the effectiveness of risk management techniques across the US Army. In early versions of the awareness raising event we described in detail the motivation for their work, illustrated in Figure 6, and showed how it might be applied within Air Traffic Management. Some participants argued that this was a distraction and that we should have the self confidence to simply promote the application of these ideas in ATM rather than create justifications based on previous research in other domains. This contradicts some of the assertions made by the proponents of action research. However, the close focus on end user requirements persuaded us to revise the course in the light of this feedback.

- ***'Distinguish between Advanced and Basic Levels of Expertise'.*** Initially, the site visits were used to identify a common set of concerns shared by various stakeholders. These initial phases of the action research technique arguably created a false impression of the homogeneity of expertise in degraded modes across European states. By identifying the shared problems in coping with infrastructure failures, we did not adequately consider the different level of skills and expertise in different ANSPs. When we visited one state, the

engineering teams had participated in a series of advanced courses on risk assessment techniques from some of the world's leading experts. Although this had not covered many of the topics about rapid risk assessment, they were anxious for more details on the integration of lightweight methods with the more formal aspects of techniques including the EUROCONTROL SAM methodology. On the other hand, it became clear during another presentation that the engineers in the audience had no previous knowledge of risk assessment at all – even though this is the bases of the Single European Skies legislative framework. We, therefore, created a series of modules that could be used interchangeably to tailor the precise content to the level of the audience – for instance, in consultation with safety managers before the material was delivered in each subsequent site.

- ***'Include Engineering and Operational Staff'.*** In the early runs of this material, we focussed on engineering teams with some participation from safety teams within ATM organisations. However, it quickly became clear that operational expertise was required to focus many of the subsequent discussions over the two day event. For instance, accidents such as the berlingen mid-air collision were exacerbated because ATCOs did not fully appreciate the impact of the engineering changes on underlying systems. During discussions about the role of a positive safety culture in combating degraded modes it was continually reiterated that more needs to be done to support effective communications between engineering and operational staff. Subsequent events benefitted greatly from the inclusion of both perspectives.

- ***'Include Senior Management'.*** Independent research commissioned by EUROCONTROL had advocated the inclusion of senior management in future safety culture initiatives. In consequence, a series of pioneering workshops were held with board level representation. Our work reinforced the findings from this related work. Several of the participants argued that senior management should attend the awareness raising workshops both because they would have been interested in the concept of lightweight risk assessments but also because they should learn more about the way in which degraded modes of operation can quickly overwhelm service provision. Balanced against these observations is that danger that engineers might be more inhibited in participating during the event if they know that senior management are present. Hence, it was concluded that a special event might be organised for management separate from the more usual meetings that were focused on engineering and operational staff.

The feedback described in the previous list led to short term changes in the awareness raising material. However, a number of longer term questions were raised. For instance, it is unclear how material of this nature might be introduced within the SESAR programme of work. Many aspects of SESAR rely upon the development of increasingly complex infrastructures with correspondingly complex failure modes. Hence, it is likely that the significance of degraded modes of operation and of safety culture in engineering will become more and more important. Another issue was that many of the states we visited wanted to reuse the material we presented at their own workshops. We had initially been anxious not to support this because we wanted to ensure some degree of consistency in the material that was presented across the engineering teams in different European states.

Further, long-term concerns focus on the ways in which ANSPs might continue to promote the concerns identified in the awareness raising event. This was difficult because we had a limited budget and focussed on addressing common concerns from the previous site visits. What we did not have was a tailored road map on how to take the concerns identified in the meetings and then turn them into medium and long term actions. This lack of a longer term strategy is also a by-product of the action research methodology. We had identified the rapid risk assessment techniques as a potential solution to some of the problems identified in the previous field research. However, we decided to discuss the application of these ideas with stakeholders during the awareness raising exercises before investing in any longer term development studies. The positive feedback from participants helped to validate this decision but also left a requirement to consider a host of additional technical details, including the relationship between light weight risk assessment techniques and existing safety methodologies.

8. Conclusions and Further Work

This paper has described how an action research methodology has been used to support the development of appropriate safety cultures in the engineering of air traffic management systems

through the development of awareness raising events about the hazards that arise during degraded modes of operation. The close involvement of stakeholders in problem definition and in the identification of potential solutions together with an iterative integration of previous research findings has helped to develop materials that have been widely praised by many ANSPs. However, this approach also created a number of problems. For instance, by focussing narrowly on engineering teams we arguably neglected the importance of communication with operational teams during the initial 'awareness raising events'.

A further benefit of the action research perspective was that we obtained immediate positive feedback in support of rapid risk assessment techniques. However, this raised a host of subsequent questions about the relationship between these lightweight hazard analysis methods and more established approaches in safety management. These issues remain to be addressed by more traditional research methodologies.

Acknowledgements

Thanks are due to Barry Kirwan and Tony Licu at EUROCONTROL who have guided this work from initial ideas through to the delivery of the awareness raising material across different ECAC states. Anyone interested in learning more about the rapid risk assessment techniques mentioned in this paper or in the safety-related training materials for ATM systems engineering should contact the authors at the email addresses given at the start of this paper.

References

R. Gordon And B. Kirwan, Developing A Safety Culture In A Research And Development Environment: Air Traffic Management Domain. In D. De Waard, K.A. Brookhuis, R. Van Egmond, and T. Boersema (Eds.) Human Factors In Design, Safety, And Management (pp. 493 - 505). Maastricht, The Netherlands: Shaker Publishing, 2005.

C.W. Johnson, Linate and □berlingen: 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, 2006.

C.W. Johnson, B. Kirwan and T. Licu. The Interaction Between Safety Culture and Degraded Modes: A Survey of National Infrastructures for Air Traffic Management, Risk Management, (11)3:241-284, 2009.

C.W. Johnson and C.M. Holloway, The Dangers of Failure Masking in Fault Tolerant Software: Aspects of a Recent In-Flight Upset Event, 2nd IET Systems Safety Conference, The IET, Savoy Place, London, UK, 60-65, 2007.

N. Pidgeon, & M. O' Leary, Organizational Safety Culture: Implications For Aviation Practice. In N. Johnson, N. McDonald, & R. Fuller (Eds.), Aviation Psychology In Practice (pp. 21-43). Brookfield, VT: Ashgate, 1994.

J. Reason, Managing the Risks Of Organizational Accidents. Brookfield, VT: Ashgate, 1997.

Susman, G.I. (1983) "Action Research. A Sociotechnical Systems Perspective". In Beyond Method: Strategies for Social Research, (Ed, Morgan, G.) Sage, Newbury Park, pp. 95-113.