The Interaction between Safety Culture and Degraded Modes: A Survey of National Infrastructures for Air Traffic Management

C.W. Johnson (1), B. Kirwan (2) and A. Licu (3),

(1) Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson, johnson@dcs.gla.ac.uk

(2) Safety R&D, EUROCONTROL Experimental Centre
Brétigny-sur-Orge, F-91222, France
http:// www.eurocontrol.int/eec/, barry.kirwan@eurocontrol.int

(3) EUROCONTROL
European Organization for the Safety of Air Navigation,
Safety Security and Human Factors Division,
Rue de la Fusee, 96, 1130 Brussels, Belgium
http://www.eurocontrol.int/esp, antonio.licu@eurocontrol.int

Abstract: This paper presents the initial results from a study into the interaction between safety culture and degraded modes of operation in European Air Traffic Management (ATM). Degraded modes occur when operators struggle to maintain levels of service even though key elements of their infrastructure have failed. Safety culture can be simply described as 'the way safety is done around here' – emphasizing that it is concerned with the realities of safety, and not necessarily what people say should be done. Although safety culture therefore deals necessarily with attitudes, beliefs and even feelings – so called 'soft' phenomena – it does not mean that these are any less important than more objective and visible safety management artifacts such as standards and procedures etc. Poor safety culture is often linked to the causes of major accidents and incidents. Recent initiatives in Air Traffic Management, including the European Safety Programme and its precursor, the Strategic Safety Action Plan, have also recognized that degraded modes of operation played a significant role in previous adverse events. Operators often reveal a high degree of tolerance for degraded infrastructures. There is a "can do" attitude, whereby staff struggle to maintain operations when it might be more prudent to reduce the level of service or even close airspace in order to maintain levels of safety. The high level objectives of this project are: 1. to identify safety cultural aspects that influence tolerance to degraded modes and 2. to identify 'best practices' that Air Navigation Service Providers (ANSPs) can apply to deal with degraded mode of operations.

1. Introduction

This paper argues that an organization's safety culture influences the procedures and practices that are used to address degraded modes of operation. These 'degraded modes' occur when operators struggle to maintain levels of service without the underlying support of key elements in their infrastructure.

1.1 Introduction to Safety Culture

The International Civil Aviation Organization argues that safety culture refers to "the personal dedication and accountability of individuals engaged in any activity that has a bearing on the safety of flight operations. It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters." (ICAO "Human Factors Guidelines for Safety Audits Manual", Doc 9806 AN/763, 2002). Safety culture has been described less formally as *the way safety is done around here* – emphasizing that it is concerned with the realities of safety, and not necessarily what people say *should* be done. The FAA's Air Traffic Organization adopts a more formal definition of safety culture; it is the "product of individual and group values, attitudes, competencies, and patterns of behavior that determine commitment to, and the style and proficiency of, an organization's safety health and safety

management" (Devine and Smith, 2007). This builds on the approach adopted by Reason (1997) and Pigeon and O'Leary (1994) in which there are 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 1 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.
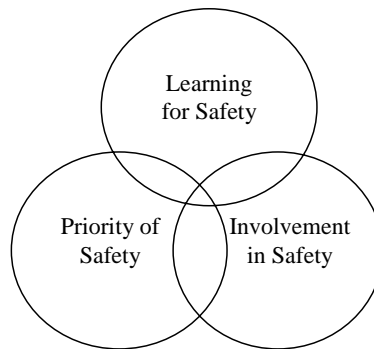
Figure 1: Components of Safety Culture

The following pages focus on the interaction between these three areas during degraded modes of operation. A deliberately broad view is adopted in which safety culture is viewed within a wider systems setting.   We are not simply interested in the attitudes and practices of ATCOs but also of management and of the systems engineers who help to maintain operating infrastructure. Most people working in safety recognize the importance of safety culture, but to some it remains vague. Its influence on operational safety can seem obscure. Similarly, safety assessors may acknowledge its importance, but have no way to model its impact in their work, for instance in safety case construction. This paper focuses on degraded modes. By looking in detail at one specific issue, readers can see how something as vague as safety culture can lead directly to operational safety problems.   Rather than the relationships between safety culture and degraded modes being vague, they are found to be complex and dynamic. Likewise, for the safety assessor who has to model the likelihood of failure or unavailability of back-up systems, this paper will provide a host of practical reasons why such applications may not be effective when needed. For the safety manager of a system, as well as for regulators of such systems and industries, whether air traffic systems or other complex systems, there are many lessons that can be learned from the detailed insights into the tolerance towards degraded modes in air traffic operations. Safety culture may be seen as a 'soft' concept, but it sometimes deals with hard issues.

1.2 Introduction to Degraded Modes of Operation
This paper focuses on degraded modes that arise when operators try to maintain levels of service without key components of the underlying systems infrastructure. They occur when part of the system continues to operate in a restricted manner, for example after the failure of data processing systems or with insufficient levels of staffing. In contrast, normal operations describe the way in which systems are designed to operate,

including planned peak periods. It can be difficult to define the precise characteristics of degraded modes of operation both within and between complex safety-critical systems. European states disagree about the list of equipment that should be available to support operators under normal conditions (Johnson and Shea, 2007). In consequence, some states would argue that the loss of a critical system would lead to a degraded mode while other states do not believe that the same component is necessary for normal operation (Shea and Johnson, 2007). We therefore face a situation in which it is difficult or impossible to develop minimum equipment lists that might be used to characterize routine operations in these industries. Rather than focus on the precise distinctions between different states, the following pages focus on the impact that safety culture has upon national infrastructures during degraded modes of operation.

It is important to place this work within the context of recent changes in Air Traffic Management. Many states both in Europe and North America are concerned to separate regulation from service provision. This provides significant benefits. For example, regulatory agencies can establish policy requirements without prescribing the means of satisfying those requirements. ANSPs, in turn, have the freedom to consider commercial pressures when selecting particular means of compliance. However, a number of problems complicate this separation of regulation and service provision. For example, it has proven difficult to recruit specialist staff to regulatory agencies. The development of independent regulatory provision has occurred at the same time as governments have increased the commercial independence of ANSPs. In consequence, many individuals have chosen to remain within part-privatized service providers rather than return to the state salary levels and promotion structures within newly established regulatory agencies. There is, therefore, a concern in some states that regulators may lack the resources and the necessary technical expertise to guide ANSPs in the development of safety cultures that increase resilience towards degraded modes of operation. A number of further concerns also motivate the work in this paper. One effect of the privatization and deregulation of service provision has been an increase in salary differentials both between ANSPS and within service providers, for instance between operations and systems support staff. Such differences can undermine attempts to establish a shared safety culture.

Further motivation comes from the reports into the two most serious ATM-related accidents in European aviation. The BFU's investigation into the Überlingen mid-air collision, argued that "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'. At Überlingen, systems and operations teams failed to anticipate the 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, problems in developing and sustaining an appropriate safety culture led to longer term degradation in the supporting infrastructures were gradually eroded. There were significant delays in replacing analogue ground movement radar systems, runway lighting systems and even ground signage were 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, 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 convicted three managers of the ANSP involved in the Überlingen accident and handed down suspended prison terms. .

2. Methods of Elicitation

Over the last two years, EUROCONTROL has developed a number of questionnaires to help Air Traffic Management organizations assess their safety culture. These include questions about attitudes to safety, for example: 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 questionnaires have been extended and tailored to local requirements for a number of service providers. A key benefit of this approach is that it is possible to assess the attitudes and beliefs of many different staff in many different functional roles across regional centers. This is important given the diversity of tasks and also the geographical distribution that characterize many ATM service providers. Questionnaires also avoid some

of the problems that arise when trying to assess attitudes to safety in group settings where individuals may be nervous about how co-workers will perceive their responses. They can also overcome some of the reluctance to discuss sensitive topics in face to face interviews with external agencies. However, the leaders of these studies recognized that a questionnaire may not be enough. Interviews and small workshops have supplemented the results from these surveys. These methods enable a deeper diagnosis of the causes of any problems and can help identify ways forward. Studies are continuing to determine whether follow-on interventions have been successful in changing processes and attitudes within service providers (Gordon and Kirwan, 2005).

The questionnaires, surveys and focus groups, described in the previous paragraphs, were not specifically intended to probe the impact that safety culture has upon degraded modes of operations. The findings of the ANSV and BFU reports into Linate and Überlingen, therefore, prompted the study presented in this paper. A key aim in starting this work was to identify the specific relationship between safety culture and issues of infrastructure maintenance across Air Traffic Management. In consequence, a series of interviews were 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 inconsistencies or inaccuracies within 24 hours of the meetings having taken place. An element of work shadowing was also possible with individual Air Traffic teams or 'watches' and with groups of systems engineers who are responsible for maintaining the underlying infrastructures. The intention was to provide a more focused analysis than the more general questionnaires. Our use of focus groups and interviews about degraded modes of operation, therefore, provided a means of complementing the results from the earlier work. It also provided highly flexible mechanisms with which to conduct this scoping exercise.

Any study of this nature inevitably involves compromises. The objective of comparing practices across different European states led to constraints on the types of methods that could be used, given the obvious political, organizational and cultural sensitivities in this area. However, this compromise approach did have the beneficial side-effect of creating a methodology that could be implemented by a single analyst working with a number of different ANSPs. This was important to ensure a consistent approach across different European states. The participating ANSPs were 'established' agencies with a strong track-record of participation in European ATM safety initiatives. They were amongst the best financed service providers in European Air Traffic Management. We were concerned to identify 'lessons learned' rather than 'blame and shame' ATM service providers. However, the traffic patterns for each site were very different. They included major providers that act as hubs for numerous regional traffic flows. Other providers operate more limited national and regional services. Current work is addressing the particular issues that face states who must maintain services in the face of rapid economic, social or political change. 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. The project described in this paper took place in three phases. These different stages each looked at different groups of service providers. The first looked at ANSPs with high volumes of traffic passing through their airspace but relatively limited amounts of domestic traffic. The second group of service providers was characterized by high volumes of both domestic traffic and over-flights. The final grouping had large volumes of domestic, regional traffic but a smaller volume of international traffic. Within these general approaches it was possible to trace a number of areas in which degraded modes of operation posed particular concerns.

3. Phase 1: High Numbers of Over-Flights and Limited Domestic Traffic
The first phase of this project looked at ANSPs with high volumes of traffic passing through their airspace but relatively limited amounts of domestic traffic. Many of these Air Navigation Service Providers distributed safety management functions across their business divisions. In the past, many ANSPs have appointed safety managers with their own specialist staff. However, it can be difficult for these centralized units to introduce changes across complex, distributed organizations. In consequence, several ANSPs have placed safety specialists directly within their various business groups. These innovations have triggered

significant culture change.   In the past, project managers felt that they had direct personal influence over key safety-related decisions. Now concern over recent accidents, including Linate and Überlingen, has led to additional layers of scrutiny.   This extension and codification of management processes has parallels in the procedures that have been developed to govern the transition between different modes of operation. For example, the decision to escalate a degraded mode into a crisis might initially be triggered by a report from an ATCO to their Shift Supervisor. They would then communicate their concerns to the duty director or Operations who would report to the Head of Center who would seek final approval from the CEO of the ANSP.   The decision to more from a 'degraded mode' into a contingency or crisis situation carries significant financial, organizational and political consequences, including significant reductions in the level of traffic.   Some ANSPs conducts regular drills and exercises to rehearse this chain of command.   In order to clarify the options available to key members of staff, the following distinctions are used by several service providers in this first group from our study:

- **Normal operation** refers to situations in which all key elements of the supporting infrastructure are functioning as intended. There may be minor faults that need to be resolved but these faults do not place undue restrictions upon the operational and systems staff as they fulfill routine tasks. Normal operation also describes situations in which periodic system updates are planned to either introduce new features or to address the minor problems that characterize everyday operation.

- **Degraded modes of operation** refer to particular problems in the underlying systems infrastructure. These are expected but are not 'normal'. Operational and system staff have well developed procedures for coping with these incidents and the risks associated with any failure are *not* perceived to be acute.   Several fault reporting systems can be used to initiate action to resolve degraded modes of operation. These modes of operation can also be associated with reduced staffing levels.

- **Crisis** refers to an adverse event that need not force a move from the operations room. Crises are more serious than degraded modes and are assumed to last for a shorter time than a contingency. The relatively severe nature of a crises means that it is handled with greater urgency than a degraded mode and actions are coordinated by the office of the director.   It is assumed that crises can be resolved within 24 to 72 hours. Examples include mid air collision, technical problems such as a data processing failure, industrial action, security incidents including bomb threats, snow, road blocks, physical isolation, acts of God (fires, earthquakes etc). Within the controllers' emergency handbooks degraded modes lead to crises or emergency situations that lead eventually to contingency plans being implemented.

- **Contingency** refers to incidents in which it is necessary to move from the standard operations room. Contingencies are likely to be more long term than crises so service continuity is a key issue.

These distinctions are important because they provide a taxonomy or ontology for labeling the state of increasingly complex and integrated systems.   In other words, management, technical and operational staff have a shared vocabulary for communicating high-level information about the overall health of the underlying infrastructure. Such a shared understanding is critical if, for instance, the concerns raised by an ATCO about a degraded mode of operation are to be effectively communicated through the intermediate management layers to those individuals who have the authority to declare a contingency or crisis. It is possible to summarize these initial findings from the first group of ANSPs in the following observation:

> **Observation 1-a:** ANSPs should develop appropriate distinctions between levels of degraded modes leading to crises or contingencies.   The process of decision making that leads to such an escalation must be rehearsed to minimize the confusion that can exist amongst both operational and systems staff over whether or not they are in a 'degraded mode', an emergency/crisis or a contingency.

Figure 2 uses the Safety Culture components from Figure 1 to group key insights from the site visits.   The three-part model provides a bridge between work on safety culture and degraded modes of operation. As

can be seen, some observations fall between different components of the three-part model. For instance, Observation 1-r deals with the need to develop systems tools to simulate complex failures under degraded modes just as operational staff have advanced simulation tools for different traffic patterns. This is grouped under 'priority for safety' because at present the existing tools for systems staff focus on reducing the time to diagnose system failures rather than helping to identify safety concerns. This finding can also be grouped under 'Learning for Safety' because it describes the development of appropriate systems training tools. Hence, it is placed at the intersection of these two components within the high-level model of safety culture.
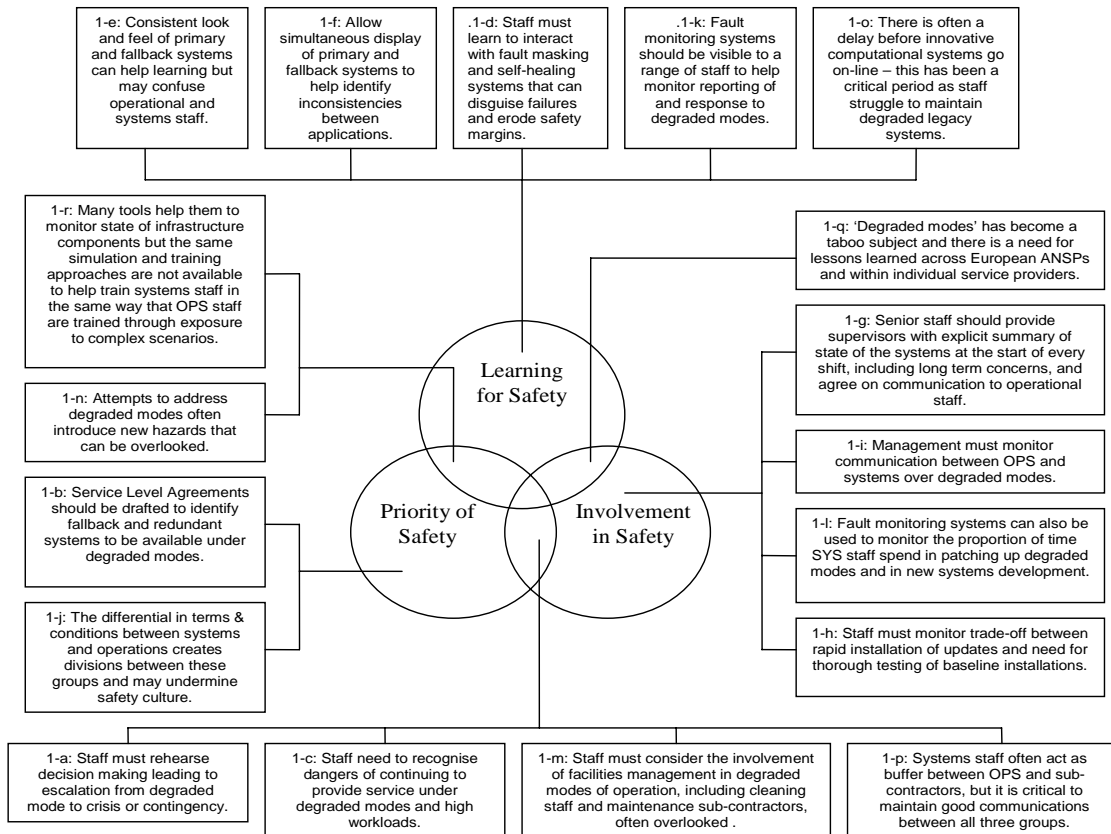
Figure 2: Overview of Safety Culture and Degraded Modes in the First Group of ANSPs

During this first set of site visits, it became clear that ANSP's also distinguish between the primary, redundant and fallback systems that are used during normal operations, degraded modes, crises and contingencies:

- **Primary Systems –** these are the elements of the ATM infrastructure that are used within normal operations. They include safety-related operational systems, such as radar, as well as 'non-essential' applications, including traffic prediction systems;

- **Redundant Systems** – many elements of the infrastructure are protected by a high level of redundancy. ATCOs can continue to use these redundant systems in the face of multiple failures to primary applications without changing their working position or moving to a fallback facility. An example would include the provision of both multiplexed and single source radar feeds. If a problem develops in the multiplexed feed then staff can seamlessly configure their systems to draw upon a subset of radar sites excluding a failing input source;

- **Fallback Systems** – ATCOs have fallback systems that can be used if primary and redundant systems fail. These fallback positions may use technology that would not normally be accepted in

primary or redundant systems because there is an expectation that they will be used over shorter periods of time until normal operations can be resumed. In other words, any risk exposure would be strictly limited. For instance, Commercial Off The Shelf (COTS) systems may be permissible in fallback systems if the costs of bespoke applications cannot be justified when many of these fallback applications will never be used.

> **Observation 1-b:** ANSPs should distinguish between the redundant systems that will be used during normal and degraded modes of operation and the fallback systems of 'last resort' that should only be used during crises and contingency. Fallback systems MUST NOT routinely be used over the longer timescales associated with either degraded modes or normal operations.

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 when 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.

> **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.

The qualitative approach taken during the site visits helped to identify concerns that might not otherwise have featured in more formal questionnaires and surveys. For example, 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).

> **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.

Primary, redundant and fallback systems often provide operational staff with different levels of functionality and support. It is, therefore, important that there are strong differences in the Human Machine Interfaces (HMI) so that staff can easily tell when they are using the primary systems rather than backup applications. However, there are strong operational reasons for keeping the HMI as similar as possible when moving between each level of support. This minimizes the training overheads that are associated with learning to use fallback and redundant systems. During the site visits to this first group of ANSPs, one of the shift teams (called 'watches') demonstrated how to change the contrast and brightness of a

fallback system so that it looked as close as possible to the primary screen. However, this undermined efforts by the systems team to distinguish between the HMI for these different levels of support. Under such circumstances there is a danger that operational teams may be confused about the level of systems support that is available in normal and degraded modes of operation.

Observation 1-e: ATCOs must be trained to recognize the different levels of infrastructure support that may be available under different modes of operation with primary, redundant and fallback systems. There is a tension between the need to maintain a *consistent look and feel* across these different levels of support because operational staff can transfer learning from normal to degraded and fallback operations. However, if the HMIs are too similar then ATCOs may forget that they are working with more limited systems support.

The ANSPs in this first phase of the project had a strong safety culture with considerable internal support for organizational safety. This is reflected in the procedures for protecting critical infrastructure. The fallback communications and surveillance systems are, typically, tested every night. One ANSP has formalized this process to that a statement is provided to the supervisor every morning to assure them about the state of the system infrastructure. Assistant controllers are available to help with technical support on a 24/7 basis. There are also systems to help ATCOs identify problems, for example, by simultaneously calling up primary and backup tracking systems to allow cross-referencing. The systematic approach to infrastructure maintenance is also illustrated by the procedures that are used to coordinate changes in the underlying systems. Offline testing and the development of system changes eventually lead to periodic updates. These are typically installed every month. Initially, the new system configuration is only operated under low loadings at night before the revised system goes 'live' for full operation. There is also a concern to avoid sudden changes in the HMI. New features are introduced gradually so that operational staff are not faced with entirely novel concepts in a single update.

Observation 1-f: Where possible it can be useful to allow for the simultaneous presentation of primary and redundant systems so that operational staff can identify the inconsistencies that are often the first warning of a degraded mode of operation.

Observation 1-g: Senior systems staff should provide supervisors with an explicit assessment of the state of the underlying infrastructure at the start of any shift. This must describe any planned maintenance and also a summary of longer term items that have still to be addressed.

Observation 1-h: There is a tension between the need to allow regular and frequent updates to baseline systems so that degraded modes of operation can be addressed in a timely fashion and yet at the same time allowing for sufficient testing to occur so that operational and systems staff can be confident in the reliability of any improvements. It is critical that ANSPs monitor this tradeoff in order to ensure that the 'peace of mind' referred to in previous observations has not been undermined.

A strong safety culture is necessary if operational and systems teams are to coordinate their response to degraded modes of operation. Simply forming mixed teams of operational and engineering staff does not guarantee that efficient and effective communications will take place. During a site visit to one ANSP in the first phase of the project, a watch described how hard it was to convince engineering support that two small failures did more to undermine confidence than one long interruption. Two failures indicate that the problem was not fixed the first time. This may seem like a trivial issue. However, previous sections have emphasized the important of confidence and trust in the operation of ATM infrastructures. The difficulty of explaining the negative impact of multiple failures is symptomatic of wider communications problems between systems and operational staff. One solution, adopted in other industries, is to encourage operational staff to train and systems engineers and vice versa. These multi-skilled individuals then understand both perspectives on the need to maintain and use underlying infrastructures. However, the differences in pay and conditions between systems and operational staff in Air Traffic Management often prevent such solutions from being adopted by ANSPs. Operational staff face significant financial losses if they moved to a systems engineering role. Instead, some ANSPs have retrained operational staff who fail to pass their operational qualifications so that they can fulfill a systems engineering role. This eases

communication but may also suggest that infrastructure maintenance is performed by individuals who would rather perform an operational role.

The importance of effective communication between operational and systems teams was reiterated across many meetings during this first phase of site visits. For instance, there are frequent problems in recruiting ATCOs and other operational staff to help with development and maintenance projects. This is a sensitive topic. The problems stem partly from pragmatic issues, including the need to coordinate development activities with operational shift patterns. However, these concerns also reflect a perception on the part of some systems teams that operational staff are not fully committed towards the associated activities that are necessary to maintain core infrastructures. The different terms and conditions between operational and systems staff may also create cultural divisions that undermine communication that is essential to address degraded modes of operation in Air Traffic Management.

Observation 1-i: Good communications are essential between operations and systems teams in order to support the repair and recovery actions that are necessary to address degraded modes of operation. It is, therefore, important that ANSPs monitor the experience of both groups when mixed teams are used on major projects. Experience in previous projects has shown that simply forming these mixed teams does not always guarantee that effective communication will take place.

Observation 1-j: There is a large and growing differential between the terms and conditions of operations and systems teams. Different pay levels and hours of service create divisions. There can be a perception in the systems teams that OPS staff do not pay the same attention to the underlying infrastructure and that some ATCOs do not contribute to the development or maintenance of safety-critical systems. Further work is required to confirm this observation and, if it is true, urgent action must be taken to address any erosion of a common safety culture.

The first phase of the project focused on staff in ANSPs with high volumes of international traffic and relatively low numbers of domestic flights. The interviews, focus-groups and work-shadowing identified a number of mechanisms to support organizational learning about the different modes of operation that were described in previous sections. These mechanisms included incident reporting systems, several of which supported on-line submission. Most of these applications were confidential rather than anonymous. Software support was also provided so that managers could browse recent reports and issue queries in order to identify common trends in these adverse events.

Observation 1-k: On-line reporting systems can be used by operational staff to submit complaints or concerns about critical infrastructure. These systems can also be used by systems teams to monitor requests for help with degraded modes. Management can use such software support to look for patterns of similar events and concerns.

Observation 1-l: On-line reporting and monitoring systems can be used to assess the proportion of time that systems teams are spending on developing new systems or debugging existing applications. Such applications can be seen as intrusive by support staff, however, they can also be used to determine whether crucial resources are being wasted on simply patching up degraded modes of operation.

Degraded modes of operation are not only affected by the interaction between operations and systems engineering teams. They are also strongly influenced by issues to do with facilities management. For example, several ANSPs record similar incidents when cleaners have inadvertently unplugged key elements of the computational infrastructure. On closer inspection, however, most of these anecdotes turn out to be unsubstantiated urban myths. There have been documented incidents where maintenance personnel have inadvertently switched off primary ATM computer systems. The first phase of site visit identified several of these mishaps. It also provided evidence of the complexity of ATM operations. Attempts to prevent systems staff from turning off active hardware, for example by enclosing them in locked units, created additional problems for maintenance staff when they eventually had to carry out scheduled maintenance and could not gain easy access to the equipment. Other aspects of facilities management must also be

considered, in particular, water ingress has affected the control rooms of several of the ANSPs that we visited in this work.

Observation 1-m: ANSPs must consider the impact of facilities management personnel on degraded modes of operation. Cleaners and technicians play a critical role in maintaining infrastructure but they can also contribute to potential hazards. Too often these groups are overlooked from initiatives to improve safety culture so it should not be a surprise when they inadvertently trigger major system failures.

Observation 1-n: Attempts to rectify degraded modes often introduce new hazards that need to be considered when conducting task analysis for key staff. For example, we have described how locked cages were used to prevent unauthorized maintenance on primary processors. These cages achieved their aim but also delayed systems staff that then had to open the boxes before they could conduct emergency maintenance.

The relevance and timeliness of this work is increased by the observation that ATM infrastructures are changing rapidly with the introduction of innovative computational techniques both to multiplex redundant information sources and also to enable rapid reconfiguration of application software. The development and application, for example of virtual networks based on Ethernet switching techniques, creates considerable opportunities for innovation and cost savings. However, these changes also create considerable technical challenges for support staff who must coordinate the introduction of new systems and also maintain existing legacy applications. There are also significant questions about appropriate means of demonstrating the safety of many novel approaches based on techniques developed for other computational infrastructures.

The complexity of technical innovation can be affected both positively and negatively through the use of sub-contracting. Systems teams are often under considerable pressure from management and operational staff to implement changes in the underlying infrastructure. However, the specialist nature of proprietary systems means that they often lack the knowledge and key resources, such as access to source code that would be required to perform these changes. In consequence, maintenance teams can be drawn into sustained dialogues with external agencies as they try to explain the changes that are needed in terms that the suppliers can understand. Resources can be wasted as communications break down between the operational teams, systems engineering and external suppliers.

Observation 1-o: Computational systems and novel network technologies enable systems teams to coordinate the rapid reconfiguration of redundant and fallback systems. However, the introduction of these novel systems can be both costly and complex. It takes time to implement innovative architectures. During this interval, legacy systems must be maintained until the new ones go on-line. Systems staff must be supported as they struggle to implement new systems and at the same time maintain legacy systems that they know will be discarded in the future. They must also respond to continuing requests for support from operational teams.

Observation 1-p: ATM service providers typically rely on a range of specialist manufacturers and systems integrators. Systems teams may not have access to proprietary source code and design information. They must, therefore, act as a buffer between operational staff requesting modifications and the sub-contractors who can implement the changes. Communications can be difficult and numerous misunderstandings can arise in ensuring that operational requirements are satisfied by external agencies.

The site visits with the ANSPs in the first phase of this study revealed considerable differences in the mechanisms that support organizational learning between the systems and operational teams. For operational staff, there were sophisticated logging and replay tools that enable supervisors and safety managers to look at the information available to ATCOs during adverse events, including AIRPROX incidents. In contrast, systems teams often lacked similar resources for organizational learning from adverse events that either led to or exacerbated degraded modes of operation. Several recent failures were described during meetings with the systems teams. However, many had become the subject of folklore. They were discussed informally but there was no formal process for integrating these previous incidents

into training and exercises.   For example, one center recently lost its radar feeds.   When work is taking place on a remote radar installation, field engineers will telephone to say that they are about to begin a maintenance task. The effects of the maintenance can then be observed through monitoring systems.   In this case the call was made in good time but the activity started before the work was logged on the monitoring system.   As the engineer worked, the feed was not disabled. False targets appeared on the ATCOs displays.   Systems staff were called to the OPS room to remedy the situation.

> **Observation 1-q:** There is a need for ANSPs to develop systematic processes for the exchange of information about previous degraded modes both internally and externally with other ANSPs.   The presence of 'degraded modes' has arguably become a taboo subject even though all ATM service providers experience maintenance issues and periodic failures. Problems may usually only be exposed to a wider audience when major accidents occur.
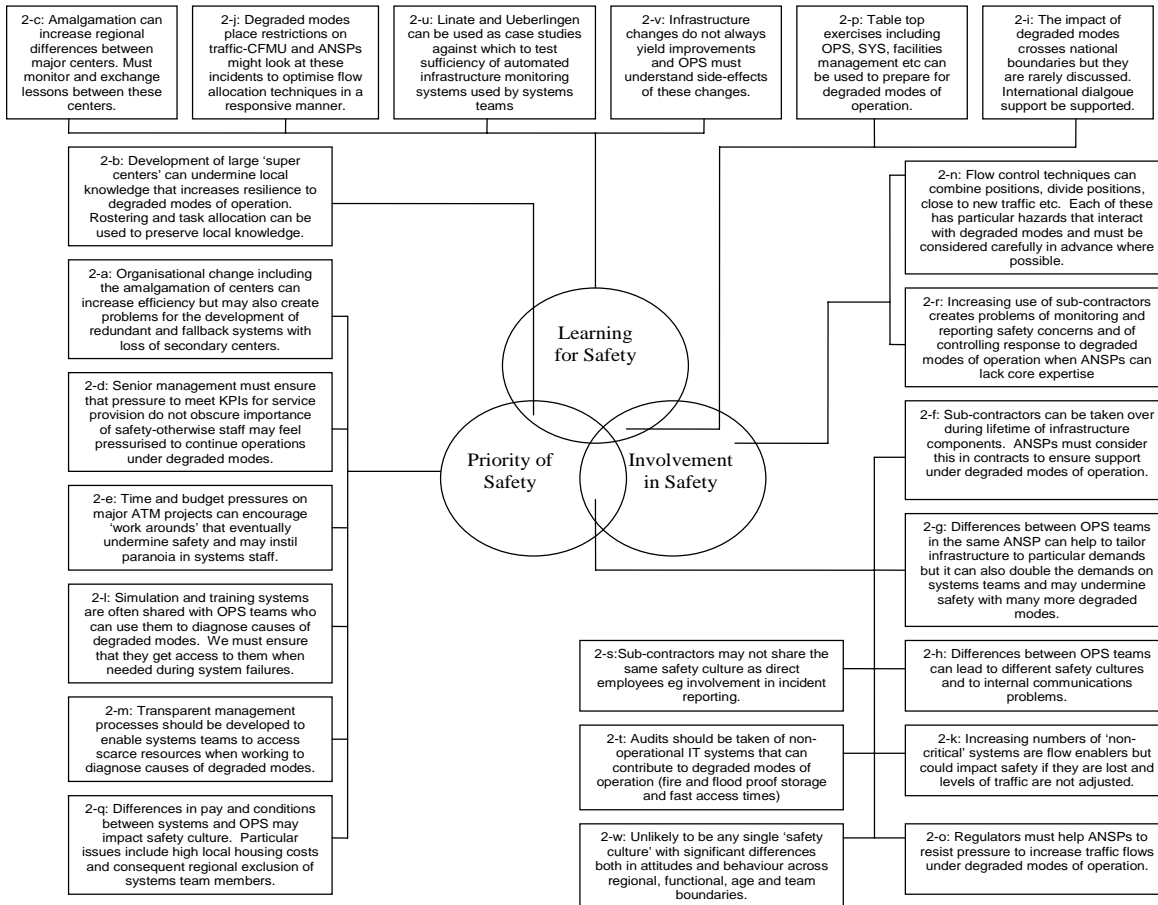>
> **Observation 1-r:** Many ANSPs have developed sophisticated monitoring and simulation tools. However, most of these have been developed to support the training of operational staff.   In the future these techniques may usefully be extended to provide systems engineers with means of logging and replaying the critical information that is presented to them during degraded modes of operation.

4. Phase 2: High Numbers of Over-Flights and Domestic Traffic

The first phase of this project looked at ANSPs with high volumes of traffic passing through their airspace but relatively limited amounts of domestic traffic. The second group of service providers was characterized by high volumes of both domestic traffic and over-flights. Most of the ANSPs in this group had strong safety records.   However, even these organizations have to face the challenges that arise when they go through organizational changes.   Several service providers visited in this second phase had recently gone through various forms of privatization. This has created expectations that they will provide a financial return to investors.   Some ANSPs were, therefore, conducting amalgamations bringing regional centers together on the same site.   It can be argued that this process of centralization is taking place more rapidly amongst this second group of ANSPs because of the relatively high volumes of traffic that they support. These amalgamations can simplify the procedures used to address degraded modes if systems teams centralize their support efforts. There is a correspondingly greater likelihood that technical experts will be available on a smaller number of larger sites.   However, the need to provide financial returns has also increased reliance on out-sourcing and sub-contracting. This affects systems teams who must work with external companies.   Any increases in the use of these arrangements can also create uncertainty over job security. Although it is not possible to infer that such uncertainty will have an impact on safety culture, it can affect other aspects of human resource management.

> **Observation 2-a:** The senior management within ANSPs must consider the impact that high-level organizational changes will have upon the management of safety within an organization.   The amalgamation of centers creates opportunities for cost savings and can also focus scarce engineering resources where they are needed most. However, these amalgamations also create uncertainty about future employment within systems teams. If they are coupled with the increasing use of sub-contracting then these concerns may be multiplied.

The generic safety culture model introduced in Figure 1 provides a high-level structure for the observations that were made during this second phase of visits to ANSPs with high volumes of both domestic traffic and international over-flights.   Figure 3 summarizes the key insights in this way.   It also captures the observation that the centralization of ATM service provision has a profound impact on wider organizational culture. There is a danger that the development of large multi-operation centers will destroy some of the team bonds that exist between watches in smaller, regional centers.   It can be difficult to encourage the development of local knowledge if ATCOs are frequently moved between sectors in large centralized facilities. Such amalgamations therefore need proactive management of safety-related knowledge (especially local knowledge) and careful management of team relationships to compensate for breakdowns in existing informal team relations. Shift patterns and workload allocations must, therefore, be carefully monitored to avoid the adverse effects of amalgamation and centralization.

2-c: Amalgamation can increase regional differences between major centers. Must monitor and exchange lessons between these centers.

2-j: Degraded modes place restrictions on traffic-CFMU and ANSPs might look at these incidents to optimise flow allocation techniques in a responsive manner.

2-u: Linate and Ueberlingen can be used as case studies against which to test sufficiency of automated infrastructure monitoring systems used by systems teams

2-v: Infrastructure changes do not always yield improvements and OPS must understand side-effects of these changes.

2-p: Table top exercises including OPS, SYS, facilities management etc can be used to prepare for degraded modes of operation.

2-i: The impact of degraded modes crosses national boundaries but they are rarely discussed. International dialgoue support be supported.

2-b: Development of large 'super centers' can undermine local knowledge that increases resilience to degraded modes of operation. Rostering and task allocation can be used to preserve local knowledge.

2-a: Organisational change including the amalgamation of centers can increase efficiency but may also create problems for the development of redundant and fallback systems with loss of secondary centers.

2-d: Senior management must ensure that pressure to meet KPIs for service provision do not obscure importance of safety-otherwise staff may feel pressurised to continue operations under degraded modes.

2-e: Time and budget pressures on major ATM projects can encourage 'work arounds' that eventually undermine safety and may instil paranoia in systems staff.

2-l: Simulation and training systems are often shared with OPS teams who can use them to diagnose causes of degraded modes. We must ensure that they get access to them when needed during system failures.

2-m: Transparent management processes should be developed to enable systems teams to access scarce resources when working to diagnose causes of degraded modes.

2-q: Differences in pay and conditions between systems and OPS may impact safety culture. Particular issues include high local housing costs and consequent regional exclusion of systems team members.

Learning for Safety

Priority of Safety

Involvement in Safety

2-n: Flow control techniques can combine positions, divide positions, close to new traffic etc. Each of these has particular hazards that interact with degraded modes and must be considered carefully in advance where possible.

2-r: Increasing use of sub-contractors creates problems of monitoring and reporting safety concerns and of controlling response to degraded modes of operation when ANSPs can lack core expertise

2-f: Sub-contractors can be taken over during lifetime of infrastructure components. ANSPs must consider this in contracts to ensure support under degraded modes of operation.

2-g: Differences between OPS teams in the same ANSP can help to tailor infrastructure to particular demands but it can also double the demands on systems teams and may undermine safety with many more degraded modes.

2-s: Sub-contractors may not share the same safety culture as direct employees eg involvement in incident reporting.

2-t: Audits should be taken of non-operational IT systems that can contribute to degraded modes of operation (fire and flood proof storage and fast access times)

2-w: Unlikely to be any single 'safety culture' with significant differences both in attitudes and behaviour across regional, functional, age and team boundaries.

2-h: Differences between OPS teams can lead to different safety cultures and to internal communications problems.

2-k: Increasing numbers of 'non-critical' systems are flow enablers but could impact safety if they are lost and levels of traffic are not adjusted.

2-o: Regulators must help ANSPs to resist pressure to increase traffic flows under degraded modes of operation.

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

Observation 2-b: Several ATM service providers are amalgamating or centralizing service provision through the closure of regional centers and the development of 'super centers'. This avoids some concerns, for instance it can reduce the differences in technical support between regional units and national control rooms. Centralization also creates other concerns including the loss of local knowledge. This can undermine operational knowledge of problems in the regional infrastructure, including radar support, that informs the response to degraded modes of operation. In consequence, considerable care must be taken to preserve local knowledge and associated team-based networks of mutual support when ANSPs centralize key resources in one or two national centers.

Observation 2-c: There is a danger that by amalgamating regional centers, ANSPs will increase the social and technical differences that exist between the smaller numbers of larger units that remain. 'They do things differently over there'.

Many of the larger ANSPs in this second phase of the project operate in regulatory environments where service charges and fee generation are closely tied to key performance indicators (KPI). These high-level requirements have a profound impact on organizations and they have been neglected by previous studies of safety-culture in complex organizations. Too often research has focused narrowly on the operational 'shop floor' without considering wider managerial influences. The use of KPIs can serve to focus undue attention on performance without adequately considering overall safety. It is the regulators task to ensure that this does not happen; by balancing safety related metrics against those of performance.

Observation 2-d: The interaction between degraded modes of operation and safety culture must be considered within the wider organizational setting. In particular, the impact of key performance indicators

on senior management decision making can help to determine the balance between safety and performance metrics. At the 'sharp end' this can persuade systems staff to implement workarounds that sustain traffic flow with increased levels of risk. Conversely, a more flexible approach to these performance indicators can enable staff to halt or reduce flow when degraded modes of operation threaten safety margins.

Just as it is important to consider the impact of regulation and key performance indicators on all levels of an ANSP, it is also important to consider the wider impact of organizational priorities on the management of degraded modes of operation. All of the air traffic service providers in this second phase of the project faced relatively high volumes of domestic and international traffic. They were also all concerned about sustaining levels of service in the face of predictions about the increasing demand for service provision. They, therefore, all had rolling programmes of major upgrades to increasingly complex infrastructures. The ANSPs in this group had all experienced delays in delivering necessary improvements. These were widely perceived to have had an adverse effect both on public opinion and on future investors. All of the ANSPs had responded by increasing pressure on systems teams to ensure project completion within predicted timescales and to budget.

Observation 2-e: Major projects within Air Traffic Management carry significant risks in terms of cost and time estimates because of the complexity of the engineering involved. There are potential risks that by stressing the continual need to work within a budget and to a particular timescale; individual engineers will feel under undue pressure. This may eventually compromise safety if the pressure for project completion encourages the use of 'work arounds' similar to those that have been witnessed in degraded modes of operation. This does not imply that there should be unlimited budgets and flexible deadlines. However, it is critical that a culture of fear does not develop in response to management pressure for project completion.

One of the ANSPs visited in this second phase has delivered a number of complex, technical innovations in its infrastructure provision. However, one recent project involved a leading international supplier of ATM software. During this contract the company decided it would no longer work in the ATM market and sold its interests to a third party. The service provider then had to negotiate with a new group of senior and middle project managers, many of whom had not been involved in the initial contract negotiations. The long term maintenance of such applications during degraded modes of operation may depend upon third party suppliers who were not involved in the initial requirements, specification and design of increasingly complex systems.

Observation 2-f: ANSPs must develop contracts that can be enforced when degraded modes of operation require prompt intervention from external companies, given that these companies may not be the original developer of safety-critical applications.

The second stage of this project deliberately focused on ANSPs that supported high volumes of domestic traffic and large numbers of over-flights. The relative scale and diversity of their operations undermined the idea that there might be a single 'safety culture' within many ANSPs. ATM service providers are complex organizations that bring together technical specialists from many different domains. Work is coordinated through different branches of operational management. In consequence, most ANSPs exhibit many distinct safety cultures which are characterized by strong regional, functional and professional differences. For instance, one ANSP simultaneously supports different procedures and technical infrastructures for area and terminal operations. The control rooms are in different locations, the layout and equipment used are also quite different. However, it is difficult to judge whether there are any systematic differences in the way in which these two groups coordinate their response to degraded modes of operation.

Observation 2-g: Internal differences within the operations of a single ANSP can ease management and operation issues – procedures and policies, as well as technical equipment can be tailored for the demands faced by particular groups of co-workers. However, there is an inevitable cost in terms of the diversity of equipment that must be maintained by systems teams in order to enable different operating environments, for example between area and terminal control.

Observation 2-h: Differences in the operational environment and working procedures, for example between Area and Terminal Control, can lead to significant differences in working practices and in culture. Further, longitudinal studies are required to assess the impact of these differences. However, it seems critical that ANSPs should identify and monitor the consequences of such organizational differences both on safety culture and the manner in which operational staff respond to degraded modes of operation.

Many of the managers, ATCOs and systems engineers visited in the larger sites during this second phase of the project argued that degraded modes of operation create problems that extend across international borders. They not only must struggle with infrastructure issues inside their own center and organization. They must also find 'work arounds' to support the changes in traffic flow that are the consequences of degraded modes in neighboring ANSPs. Several teams referred to the lack of dialogue that goes on in this area. They argued that these problems are, typically, only considered in the aftermath of accidents such as Überlingen. They suggested that such dialogues must be extended so that systems engineers, in particular, can share lessons learned and best practices across national borders.

Observation 2-i: Degraded modes of operation have knock-on consequences that extend beyond national boundaries. ANSPs must deal with the consequences of failure in their own systems but also the knock-on effects from other states. However, these issues are seldom discussed between national service providers except in the aftermath of major accidents.

Most of these larger service providers did not distinguish between normal and degraded modes of operation using minimum equipment lists. Each system failure is identified as soon as possible. Systems staff must then identify any associated repairs and establish replacement deadlines to rectify any short comings. These schedules are subject to the same project management constraints of cost and timescale that were emphasized in previous paragraphs. Particular problems can arise when degraded modes place flow restrictions on routes that provide the main transport infrastructure for remote communities. For example, several of the ANSPs supported domestic flights where there were no feasible alternative means of transport for outlying communities. We will return to this these in the next section, which reports on service providers that focus on national and regional infrastructures.

Observation 2-j: There is a need for international agreement on the procedures and processes to be used to allocate any residual capacity when degraded modes of operation jeopardize critical infrastructure flows to remote communities.

Most of the ANSPs in the second phase of this project use risk assessment techniques to identify the importance of primary and secondary systems. This is important because there are considerable costs associated with the interruption to either domestic or international services. For instance, several service providers argue that flow prediction systems are relatively low risk and staff should, therefore, not need secondary or fallback applications. These systems are intended to help controllers to anticipate the movements of aircraft using flight plan information, aircraft type, meteorological conditions etc. They are not, typically, considered essential because service provision can continue even when they are unavailable. In contrast, radio telecommunications systems are assigned the highest level of risk. Service provision cannot, typically, be sustained without this infrastructure and so operational staff are provided with both secondary and fallback communications systems. However, it can be difficult to apply risk assessment techniques to identify the criticality of infrastructure components during degraded modes of operation. Although flight prediction systems are not viewed as essential, they do have a considerable impact on capacity. It can be argued, therefore, that the loss of such systems would lead to a degraded mode of operation. During this time it may be necessary to prevent departures and simply focus on what is currently in the air. Such examples illustrate that degraded modes do not simply relate to 'essential' infrastructure but also to capacity enabling systems.

Observation 2-k: For non-critical operational systems, it is important that ANSPs consider the impact that the loss of such a system would have upon the capacity of a center. An increasing number of systems are flow-enablers. If these systems go down then not only will the center be operating in a degraded mode but

safety will also be threatened if management and supervisors fail to reduce workload to an appropriate level.

Several of the ANSPs in this phase of the project had extensive resources for training and development. Banks of workstations were available to systems engineering teams so that they could pre-install and debug software updates. These resources support end-user trials and more complete simulation exercises. Engineering teams can also use them to diagnose the causes of degraded modes. Modifications to existing applications can be trialed to see if particular changes will resolve operational problems. However, this is only possible when the duplicate resources can be reconfigured so that they accurately reflect the systems that are installed on primary workstations. Several of the service providers had, therefore, developed informal agreements to ensure that training and simulation systems could be reconfigured back to the version in operations rooms within a specified period of time. The site visits did not identify more formal, written agreements.

Observation 2-l: ANSPs often have access to training and testing applications. These facilities provide important benefits for degraded modes of operation because staff can use them to diagnose underlying faults. This can be difficult if development activities go well beyond current configurations in the operations rooms. ANSPs should, therefore, draft internal procedures to ensure that these scarce resources can be reconfigured during degraded modes of operation.

The workstations and networks that support training and development are scare resources. They support systems engineering activities. They can also act as replacement positions when technical failures or terrorist actions compromise primary systems. In such circumstances, the training and development resources cannot be used by systems teams in order to diagnose the causes of any failure. In other words, a critical part of the development infrastructure will be used to provide backup control systems and hence cannot be used to diagnose the original failures. Similarly, ATCOs will not be able to run simulations of degraded operating procedures if simulators are being used as primary control systems. The pressure for shared-use infrastructures comes in part from the need for part-privatized organizations to maximize returns on investment. Different groups compete for access and it is not clear that safety-related issues will always be the primary concern – nor is it clear what criteria might be used to decide between two sets of potential users that are working on safety related problems.

Observation 2-m: In situations where there is competition for the scarce resources needed to diagnose and resolve degraded modes of operation, it is important that ANSPs provide a process for ensuring that safety related concerns have priority over, for instance innovations in capacity management. Equally where a case can be made on safety grounds for access by one or more teams then criteria should be developed to preserve cooperation between the different groups accessing a shared resource.

Several of the service providers in the second phase of the project dealt with degraded modes by placing restrictions on the traffic that enters particular sectors. Alternatively, sectors can be further divided to ensure that the controllers' workload is well matched to the resources that they have available. There are, however, limits on the use flow control as a means of ensuring safety during degraded modes of operation. Additional sectors can only be created if trained staff are available. Sub-divisions can only reasonably be implemented up to a finite level of granularity before there is a loss in overall situation awareness, for example on the approach to major airports. The ability to train ATCOs and to maintain expertise across multiple sectors and positions is also limited. For example, one of the phase 2 ANSPs cannot easily reallocate staff to support the major national airports in their areas because these have reached a level of complexity where dedicated controllers can take many months to become familiar with the patterns of traffic. The regulator is ultimately responsible for ensuring that the level of traffic is well matched to the infrastructure resources that are available under degraded modes of operation. However, this is a very difficult task given that there will be strong economic pressures to maximize service provision. The ANSP therefore, assumes that there will be a gradual build up to full capacity after flow has been cut to reduce the impact of any degraded mode. Capacity will only be increased once the stakeholders agree that it is safe to do so. This implies that there is strong management support not to arbitrarily increase load before it is safe given considerable commercial pressures.

Observation 2-n: Flow control techniques can be used under degraded modes of operation so that workload is reduced when key elements of critical infrastructure are no longer available. One means of doing this is to close the sector to new traffic or to place tight restrictions on the slots that are available. Alternatively, sectors can be subdivided to isolate problems and to share workload between multiple controllers. However, there are dangers with each of these approaches. For example, the subdivision of sectors can undermine overall situation awareness in complex positions. Considerable care must also be taken to ensure that safety is not compromised by the level of traffic that is to be supported under degraded modes. In the extreme, it should be possible for ATCOs to close a position if they are concerned about the level of work that they must perform under degraded modes.

Observation 2-o: Regulatory and management support is essential to restrict the pressure that can be placed on ANSPs and operational staff to resume normal levels of traffic during any degraded mode.

Several of the ANSPs in phase 2 have conducted exercises to plan their response to degraded modes of operation. These meetings involved stakeholders from a range of different groups including operational teams, shift supervisors, control room management, systems teams, systems supervisors, safety management and sub-contractors. Regulators were not, typically, included. However, several of the service providers described the inclusion of facilities management in this exercises. They confirmed the phase one observation about the importance of these teams. An important issue for the phase two ANSPS was whether or not they owned their site. In some states, it had proven to be difficult to commission repairs to the physical infrastructure when service providers did not have direct ownership of the buildings where they worked.

Observation 2-p: ANSPs conducts tabletop exercises with mixed groups of operations and systems teams, as well as facilities teams and different levels of line management. These exercises use previous experience of degraded modes to plan for future system problems. They provide significant benefits; in particular such meetings can support communication about the detection and resolution of system failures.

Previous sections have described some of the problems that can arise when different safety cultures emerge between the teams who maintain infrastructure and those who must operate it. These tensions can be exacerbated by significant pay differentials between systems and operations. However, this is not the only source of tension. For instance, even relatively small differences in remuneration can lead to informal 'segregation'. Systems engineers may not be able to purchase housing in the same areas as operational staff. In extreme cases they may have to commute significant differences to operational centers, limiting opportunities for social interaction with co-workers. It cannot be argued that this has a direct impact on safety. However, pay and conditions can influence staff retention in both systems and operational teams.

Observation 2-q: Some ATM centers are located in areas with high relative housing costs. This can create problems for systems teams if they cannot afford to live close to the centers that they help to maintain. ANSPs must not be afraid to monitor and address these issues.

The use of out-sourcing can yield significant cost savings. It can also create considerable problems for addressing the root causes for degraded modes of operation. For example, one manager in a phase two ANSP described a problem in persuading their sub-contractor to demonstrate communications facilities. The sub-contractor's position was reasonable given the context of the request that was made to them. In order to test the facilities they would have had to obtain radio frequencies that were being used by operational staff. If the sub-contractor had been part of the ANSP's organization then such a request might have been relatively easy to meet. However, it was difficult for the external organization to identify the person in the ANSP who had the technical knowledge and appropriate authority to approve their request. Most degraded modes of operation are the result of faults that trigger longer term or latent issues in the design, operation or maintenance of complex systems. This creates problems for the more devolved management structure of some ANSP organizations. In particular, the use of multiple sub-contractors implies a need to communicate with the 'right people' in several different companies in order to resolve many degraded modes. One sub-contractor may be responsible for cabling and installation of

communications infrastructure while another holds the maintenance contract for these resources. **It is, therefore, important that suppliers must share an appropriate safety culture with the ANSPs.**

Observation 2-r: ANSPs have made increasing use of external organizations and sub-contracting to meet key system requirements, including maintenance and support. This delivers considerable savings. However, it also raises important problems in establishing effective communication. It can be difficult for the sub-contractor to identify the personnel in the ANSP that have the authority and technical knowledge to address their concerns – for instance, who should a sub-contractor approach to rectify a fault or to report problems with key members of staff?

Observation 2-s: Sub-contractors are being used in many different areas of Air Traffic Management. **This creates concerns because the employees of these companies may not share the safety culture that is being nurtured within ANSPs.** Basic communications mechanisms must be established to ensure that each party understands the extent of their responsibilities when attempting to resolve adverse events, including degraded modes of operation.

Several of the larger ANSPs in the second phase of the project have begun to consider the influence that non-operational IT systems have upon degraded modes of operation. They have recognized the dependencies that exist between operations and infrastructure that seems to have little or no relevance to system safety. Examples include a wide range of support documentation that may be essential to rectify a degraded mode. These non-operational resources also include configuration data that would be necessary to rebuild infrastructure following incidents that affect on-line backups. A related issue is the storage mechanisms that are used to safeguard critical information resources. Backups for critical data are, typically, held at off-site locations in fire-safe structures. However, it can take some ANSPs more than 48 hours to retrieve their own data from these secure sites.

Observation 2-t: Audits should consider the impact that the 'non-operational IT infrastructure' has on degraded modes of operation. Action should be taken to ensure that systems teams have access to backups in off-site, fire/water-proof locations which can be accessed with minimal delays following an adverse event. The need to audit non-operational but safety related information is indicative of a wider need to shift the culture within ANSPs to look beyond the operations room, in order to identify wider systems risks under degraded modes.

The second phase of the project identified several innovative 'non-operational IT systems'. These included an application that enables systems engineers to send ATCOs real-time status messages about infrastructure components. Warnings can be presented on controller's workstations whenever the telecommunications systems are degraded. Operational staff can then use another system to view the reasons for any degraded modes. This application also provides information about the predicted duration for any interruption in the underlying infrastructures. Logs enable operational staff to review recent warnings when they first come on shift. This supports 'situation awareness' during the hand-over between watches.

Observation 2-u: Several ANSPs have developed innovative applications that enable ATCOs to obtain a snapshot of information about the underlying status of their infrastructures. However, it is unclear whether real-time alerts and status logs would have been sufficient to help the controllers at Zurich or Linate to avoid accidents in 2001 and 2002. These case studies could be used in validation exercises to determine whether operational staff have sufficient information resources to assess the impact of degraded modes on their operations.

Several of the managers who were interviewed in the second phase of the project were anxious not to introduce new systems unless they had clear operational benefits. For example, one of the ANSPs uses backup cabling that was initially developed in the 1940s and remains serviceable. Equally, they recognized the need to update key elements of the infrastructure. One reason for their emphasis on an evolutionary approach is that upgrades do not always achieve the anticipated benefits. This can lead to 'normal' situations that ATCOs and systems staff criticize as being degraded. For example, there is often a delay in

establishing point to point communications across digital networks. During several site visits, these new communications systems were criticized because they did not provide instant access.

> **Observation 2-v:** It is important to recognize that upgrades to infrastructure do not always yield the operational benefits that might be anticipated. In such circumstances, it is important to explain to operational staff that these features are to be expected and need not reflect underlying problems that may characterize degraded modes of operation.

As mentioned, the ANSPs in phase two tended to be larger than those in the other stages of this project. Partly in consequence, staff referred to strong differences between those major centers that remained after recent amalgamations. These differences included variations in procedures. They also included different attitudes towards safety. These regional differences were compounded by different safety cultures within watches at the same center. Most ANSPs operate a form of shift rotation where the same teams operate at different times over a four or eight week cycle. Not all members of a watch are needed during all duty periods. Only a subset of the watch are needed during the reduced traffic flows in night operations. In consequence, some members may be temporarily assigned to other watches. This can be unpopular because the ATCOs seconded to another watch will not have been through the same training sessions as their hosts. They may be unfamiliar with their style of operation even if the underlying procedures are the same. Some watches prefer to amalgamate sectors so that staff can get more breaks under rotation. Others prefer to share the work and keep a lower pace throughout the shift. The concerns over shift rotations between teams illustrate the degree of team cohesion that builds between the individuals in a watch. They are also suggestive of differences in approach that may be significant in terms of safety culture, risk taking and decision making.

Many ATCOs and managerial staff were recruited during periods of rapid expansion in the aviation industry. In several member states, this occurred during the mid-1970s. One consequence of this is that key personnel in both the operations and systems areas are about to retire. This will leave an important gap in the human resources of many service providers. It remains to be seen if this change in generation will have any significant impact on attitudes to safety. In some respects, the younger generation of controllers seems to have a heightened awareness of risk assessment but with less experience of the range of operating techniques that might be used under degraded modes.

> **Observation 2-w:** It is often misleading to talk about a single 'safety culture' within an organization as complex as an ANSP. A number of different sub-groups can be identified with varying attitudes to safety related issues. These sub-groups reflect regional differences between major centers. They also form around the watches and other small groupings of co-workers who organize their tasks in different ways within the same procedures. There may also be different safety cultures across the age profile of ANSP staff. This is particularly important given the demographics of many service providers.

5. Phase 3: High Numbers of Domestic Flights and Limited Over-Flights

The first phase of this project looked at ANSPs with high volumes of traffic passing through their airspace but relatively limited amounts of domestic traffic. The second group of service providers was characterized by high volumes of both domestic traffic and over-flights. This final grouping support high volumes of domestic and regional traffic but a smaller volume of international over-flights. Several of the service providers in this third phase of the project are widely acknowledged to have been at the forefront of recent safety initiatives. However, they face very different traffic patterns to the service providers covered in previous sections of this paper. In particular, they service a far greater proportion of operations in relatively remote areas.

Figure 4 summarizes observations from this last set of site visits. These include the uncertainty created by the potential impact of new architectures for ATM service provision. The European Commission (2004, 2004a) has issued a: "Mandate on Support for Establishment of Functional Airspace Blocks (FABs)". FABs support airspace structures that are based on the predominant traffic flows. They can, therefore, be significantly less complex and are arguably easier to operate than existing legacy structures based on national airspace boundaries. The EC plans support the Single European Skies concept. The intention is to

encourage regional cooperation and address the predicted rise in demand for ATM services. The introduction of Functional Airspace Blocks may reduce the impact of degraded modes of operation within an ANSP, for example by helping them to call on assistance from other states that are allied to that FAB. However, the plans have increased insecurity amongst personnel who fear significant changes in their jobs and in their longer term career security.
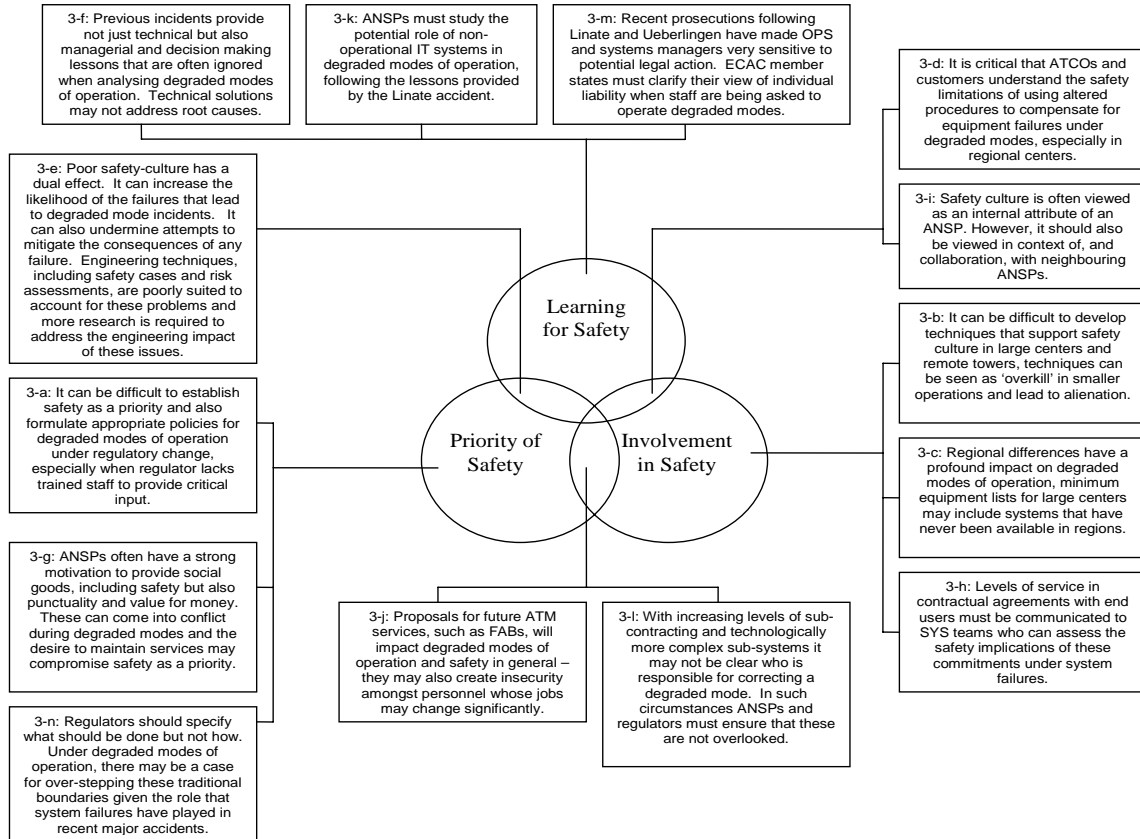
Figure 4: Overview of Safety Culture and Degraded Modes in Third Group of ANSPs

The ANSPs that were visited in this third phase of the project must, typically, support lower levels of traffic than those in the first two stages of our work. This has isolated them from some of the changes that have taken place in other service providers. In consequence, several ANSPs have only just separated their operational divisions from regulatory functions. It has been difficult to persuade the best technical staff to transfer into newly independent regulatory divisions. Remaining in government service usually implies lower salaries than those offered by newly independent service providers. Regulators, therefore, often lack significant expertise in core technical areas. This can result in delays before detailed policy can be drafted for areas including the appropriate response to degraded modes of operation.

Observation 3-a: It can be difficult for ANSPs to identify appropriate policies to support the development of a strong safety culture and to establish effective procedures for dealing with degraded modes of operation in a climate of regulatory change. They must rely upon internal monitoring and audits. At the same time, this uncertainty can also make it difficult for regulators to recruit well qualified managers and engineers. Under such circumstances, it is particularly important that ANSPs document the steps that they have taken to address the issues of safety culture and degraded modes of operation in a way that is transparent to external inspection.

Several of the ANSPs in this final phase of the project provide air management services to out-lying airports in more remote regions. Staff in these sites operate with a high degree of independence. Low

traffic levels enable the development of procedures and practices that would not normally be acceptable in other operational contexts. They also benefit from the relatively stable nature of air traffic in these regions. Under degraded modes of operation, it is often possible to develop conflict-free or nearly conflict-free routings at lower capacity.

> **Observation 3-b:** The geographical distribution of some ANSPs makes it hard to maintain a common corporate safety culture in both national centers and regional airports. Methods developed for large centers can be 'overkill' in smaller regional units. However, the events at Linate accident show that this culture can be dangerous when changing traffic patterns expose informal operating practices. ATCOs and systems engineers must be made aware of these potential dangers to demonstrate that safety culture is relevant in the regions and not just in national centers.
>
> **Observation 3-c:** Regional differences in the nature of operations, of traffic loads and of technical support also create differences in the potential degraded modes of operation that will affect ANSPs. Minimum equipment lists cannot easily be applied across diverse operating environments, when systems that are essential for a national center have never been available in remote centers. Hence any analysis of the interaction between safety culture and degraded modes must be sensitive to the different demands and resources that are available.

The provisions for degraded modes are quite different in regional centers visited in phase three compared to the larger national sites. The higher level of traffic at major centers, typically, justifies a greater level of investment in the technical systems that support redundancy and fallback operations. However, the staff from regional units often argue that they can continue to operate safely without the support of fallback systems, although this implies significantly reduced capacity. Smaller towers prepare for the loss of systems, including radar, VHF, UHF, that would close the national centers. Relatively stable traffic patterns enable many regional operations to be conducted using the absolute fallback procedures ensuring 20 miles and 5,000 ft separation. However, it is important not to exaggerate the degree of protection that lower workloads and stable traffic patterns can provide for degraded modes of operation in regional centers. For instance, regional operations are usually focused on a small number of airspace users. ANSP staff also tend to have close personal relationships with airport management. In such circumstances, considerable pressure can be placed on individuals to find 'work arounds' for degraded modes.

> **Observation 3-d:** The lack of redundant and fallback systems in regional control centers makes it important that ATCOs understand the limitations of procedures that can be used to maintain services when critical infrastructure is lost. It is also extremely important the customers and colleagues, including regional airport managers, understand the hazards that can arise under procedures that enable local airports to remain open during degraded modes of operation.

It can be argued that the relatively small scale of several of the third phase ANSPs has helped them to develop flexible and innovative safety policies for degraded modes of operation. For example, most regulatory organizations require that primary systems are justified by an appropriate safety case. However, there is no corresponding argument to document the safety of fallback systems in the majority of the service providers that were visited in this project. However, the third phase ANSPs has begun to extend their safety case development to consider both secondary and fallback applications. As part of this work, they had identified a number of technical problems in developing appropriate risk assessment techniques when it is difficult to predict the circumstances in which secondary systems would be needed. For example, safety cases can be based on the argument that the increased residual risk from the use of fallback systems will be limited in terms of any foreseeable exposure. In other words, it is acceptable to rely on reduced levels of support if these systems will not be operated for long. However, in order to quantify such a reduced exposure it would be necessary to assess the probability of these systems being required and also to estimate the time needed to restore primary applications. Given the nature of the hazards that we face, in terms of terrorist incidents as well as technical failure, it can be difficult to validate any risk assessments based on such calculations.

Observation 3-e: A strong safety culture must be supported by appropriate technical and engineering processes. Safety cases have been developed for primary systems. However, these often fail to capture the precise circumstances that arise during degraded modes of operation. There are also problems in validating risk assessments that cover relatively rare incidents, particularly when those incidents themselves may be influenced by flaws in the underlying safety culture.

The final phase of site visits confirmed some of the observations that had been made at the other centers. Most of the primary systems in major national centers are extremely reliable. For example, one of these regional ANSPs reported a single 'serious' problem in the last two years. However, the relatively low number of major failures creates problems when staff are eventually exposed to degraded modes that have not been foreseen in exercises and drills. In this example, the operations teams responded to the failure by transferring traffic from the failing center to other national facilities. However, it was not technically possible for these neighboring centers to take over the airspace controlled by the failing site. There is a plan to address this by providing redundant hardware in each of the major national centers. However, it is also recognized that such 'upgrades' in fallback provision will not be the 'final word'. Continual development is necessary to improve or modify plans in response to changes in the air navigation systems. As primary systems become more sophisticated then so must the secondary and fallback applications. If too great a gap develops between these different layers of redundant systems then staff may not be able to use the applications that are provided to combat degraded modes of operation when primary systems fail.

Observation 3-f: In a strong safety-culture, previous failures provide learning opportunities. However, they are also symptomatic of previous weaknesses. Hence it is not sufficient simply to install the technical equipment that might prevent any future recurrence without also assessing the management and decision making processes that arguably led to the failure in the first place.

Several of the ANSPs, which participated in this final phase of the project, have a long history of innovation in safety management, often in conjunction with labor representatives. Given their regional focus, they have a strong social concern to maintain services for remote, outlying communities. They also place considerable importance on consultation with wider stakeholders including the regulator. However, the managers in these service providers described consider difficulties in establishing any consensus over the best ways to prepare for degraded modes of operation. The higher the reliability of ATM operations, the harder it is to convince airspace users to make additional investments into the underlying infrastructure especially for scenarios that have not affected service provision in the past. It can also be difficult for ANSPs to judge the investments that should be made in preparing for adverse events in remote regions given that the strategic impact of any interruption to services may be far more profound than the economic costs associated with the loss of ATM operations in those regions.

Observation 3-g: ANSPs must consider the social context of their operations when planning to combat degraded modes of operation. For example, government and public concern may encourage service providers to resume operations to remote regions as soon as possible given that air traffic may provide vital links to these communities. However, these wider concerns must be balanced against the ANSP's need to ensure profitability during the recovery from any adverse event.

There is often an assumption that an appropriate safety culture should place the highest priority on safety. However, the interpretation of this statement raises important questions within Air Traffic Management. For example, one of the ANSP that participated in the final stage of this project has en route charges that are almost half those of their neighbors. These charges reflect the demand for services across different adjacent sectors. These differences in revenue imply that it will be difficult for all ANSPs to afford the same level of redundancy across their different technical infrastructures. Additional revenues can be used to support additional investments in secondary and fallback systems that cannot easily be justified by the lower levels of traffic in many of the ANSPs that were visited in the third phase of this project.

Airspace users often have little idea about the different levels of infrastructure provision that exist between ANSPs. Many of the service providers that participated in all three phases of this project were anxious to increase the dialogue about degraded modes of operation with the organizations and companies that pay for

their services.   Such dialogues can be hard to initiate and to sustain.   It is difficult to assess attitudes across the range of customers for ATM services including airlines but also military users, individual airports, the International Air Transport Association, the International Civil Aviation Organization etc. Further uncertainty about support for degraded modes extends to those who are employed by many ANSPs. Operational, managerial and systems staff all expressed some confusion about the levels of service that their organizations were contracted to provide to airspace users.

Observation 3-h: ANSPs should conduct a systematic review of the levels of service both anticipated by and contracted to end users. The findings of such a review should be communicated to the staff who are involved in planning for service cover under degraded modes of operation.

Several of the ANSP in this final stage of the project have letters of agreement for mutual support from neighboring countries under both degraded modes and contingency operations.   However, the procedures and protocols that support these high level initiatives are largely untested except in the informal load balancing that is part of everyday cooperation between service providers. The development of FABs will increase the scope of these international agreements.   In addition, there are new initiatives to provide backup services between groups of ANSPs that use the same underlying systems.   This, in theory, will expand the possibility of mutual assistance during system failures. However, previous initiatives have failed to deliver the detailed mechanisms and procedures to back-up high level agreements.   Some service providers questioned the ability of other states to handle their own everyday operational problems far less take some of a neighboring state's load during degraded modes of operation. Operational and systems teams expressed concern that their neighbors seem to be suffering increasing numbers of infrastructure failures and that this is pushing more and more traffic into their sectors.

Observation 3-i: Neighboring states can help ANSPs by taking traffic during degraded modes of operation.   This assistance must be codified in letters of agreement. Hence it is appropriate for ANSPs to form alliances not only with neighbors but also with those service providers who operate similar system architectures.   These procedures must be practiced and simulated if they are to be used successfully.

The development of FABs will resolve a number of technical issues while at the same time creating strategic vulnerabilities for the ways in which ANSPs do business. In terms of systems provision, functional groupings provide greater integration. This will help ANSPs to call for support from other member states during degraded modes.   There is a concern, however, that many ANSPs will resist the full implementation of FAB. There may be a reluctance to surrender 'national sovereignty' or to loose control of strategic assets.   The proposed changes may also lead to rationalization and the closure of existing centers. A particular concern here would be a situation in which a rival ANSP lowered their costs by removing all redundant and fallback systems. They could then acquire traffic from partner sites, safe in the assumption that their neighbors would assist them during any degraded mode.

Observation 3-j: Proposals for the future shape of ATM service provision must consider both the benefits that techniques such as functional airspace blocks provide for degraded modes of operation. They must also consider the insecurities that these plans create for service providers that fear competition from ANSPs with lower investments in safety and hence lower costs.

One benefit of focus groups, interviews and workplace shadowing is that they often identify wider stakeholders with an interest in the relationship between safety culture and degraded modes of operation. These groups can be overlooked in the sample populations for more formal surveys.   For example, we were contacted by the team responsible for aeronautical information products during a site visit to one of the third phase ANSPs. This group were trying to assess the impact of disruptions to the dissemination of their products over the web. They were also concerned to address any systemic problems that might affect the validation of the information that they provide to the aviation industry.   The complex nature of the processes used to establish consistency across these information resources is an area of investigation in its own right. It is clear, however, that their work on degraded modes of operation has strong similarities with the concerns over non-operational IT systems that were raised during the first two phases of this project.

> **Observation 3-k:** It is easy to underestimate the critical importance of non-operational documents. Many are not covered by the same quality control procedures that affect operational information resources. Similarly, it is important that ANSPs identify the range of information resources that affect the safety of ATM operations. This is illustrated by the key role of maps and plans during the Linate runway incursion.

The final phase of site visits reiterated the need to engage with a wider range of stakeholders in order to address the problems created by degraded modes of operation. For example, many states devolve responsibility for the implementation of health and safety legislation. The government bodies that oversee the implementation of these laws are responsible for coordinating potential prosecutions in the aftermath of any accident. They are independent of the regulatory bodies that oversee the more technical aspects of Air Traffic Management provision. Health and safety agencies are also, typically, kept separate from the bodies that promote aviation transportation for and within government. This separation of interests can create confusion for ANSPs, which must identify the agency that is responsible for monitoring the integrity of national infrastructures.

> **Observation 3-l:** Many degraded modes occur not from catalytic failures in particular pieces of equipment but because of administrative problems in identifying those agencies that are responsible for guiding key decisions in complex, state regulated industries. Whenever such problems occur, ANSPs should take the lead with regulators in ensuring that their infrastructure does not become degraded through inaction.

Many of the employees in the third phase of consultations were unsure about the liability of individual ATCOs using fallback systems and procedures. During degraded modes and contingency operations, staff are faced with rising workloads and by additional stress. Dealing with these pressures is part of the training and everyday experience of ATCOs. It is important to emphasize, however, that there are limits to the ability of personnel to adapt under degraded modes. Some centers are more complex than others. Differences in sectorization and traffic flows can be compounded by changes in the number of staff. All of these factors are exacerbated by the loss of critical infrastructure.

> **Observation 3-m:** Recent prosecutions of ATCOs and ANSP management following the Linate and Überlingen accidents have created considerable uncertainty about the liability of staff working under degraded modes of operation. States should take steps to reduce this uncertainty by publishing clear statements of individual liability to ANSP staff, wherever this is possible.

Regulators play a critical role in reducing the uncertainty mentioned in the previous paragraph. They help to establish the context of what should be done to prepare for degraded modes of operation. Typically, this involves the publication of objectives and recommended processes without necessarily describing in detail how ANSPs will meet regulatory requirements. One example of this is that way in which ATM regulators advocate the use of incident reporting systems, which are a foundation for strong safety cultures. Many of the ANSPs that were visited during this final phase of the project have confidential but not anonymous reporting systems. This enables analysts to go back and confirm the technical and organizational circumstances of any adverse events. However, there are often mechanisms to protect the identity of potential contributors. For example, some ANSPs appoint mediators who can act as go-betweens.

> **Observation 3-n:** It is difficult for regulators to become involved in many of the issues that affect degraded modes of operation and safety culture without transgressing the traditional boundaries between setting objectives and specifying means of implementation. This would include the precise facilities to be offered by confidential reporting systems but also includes the detailed design of redundant and fallback systems.

6. Conclusions and Future Work

This paper presents an overview of the interactions between safety culture and degraded modes of operation within Air Navigation Service Providers. A qualitative approach has been used to supplement the questionnaires and surveys that have previously yielded insights into safety culture maturity within service providers (Gordon and Kirwan, 2005). In contrast, to this earlier work our focus has been less on the wider issues to do with safety culture. Instead we have looked that the issues and concerns that arise from the detection of and response to failures in critical infrastructure. Interviews, focus groups and work

shadowing identified concerns about degraded modes from a broad range of stakeholders including senior and middle management, operational staff, systems teams and sub-contractors.   The findings from three different groups of ANSPs have been summarized in this paper.   These groupings reflect significant differences in traffic.   We have contrasted service providers with high densities of international and regional flights to those with relatively low numbers of over-flights but strong regional and national networks and also with ANSPs that support high volumes of international flights but with relatively limited domestic and regional markets.   A number of key observations have been graphed for each of these groups, shown in Figures 2, 3 and 4, using a high-level model of the components of strong safety culture, illustrated in Figure 1.
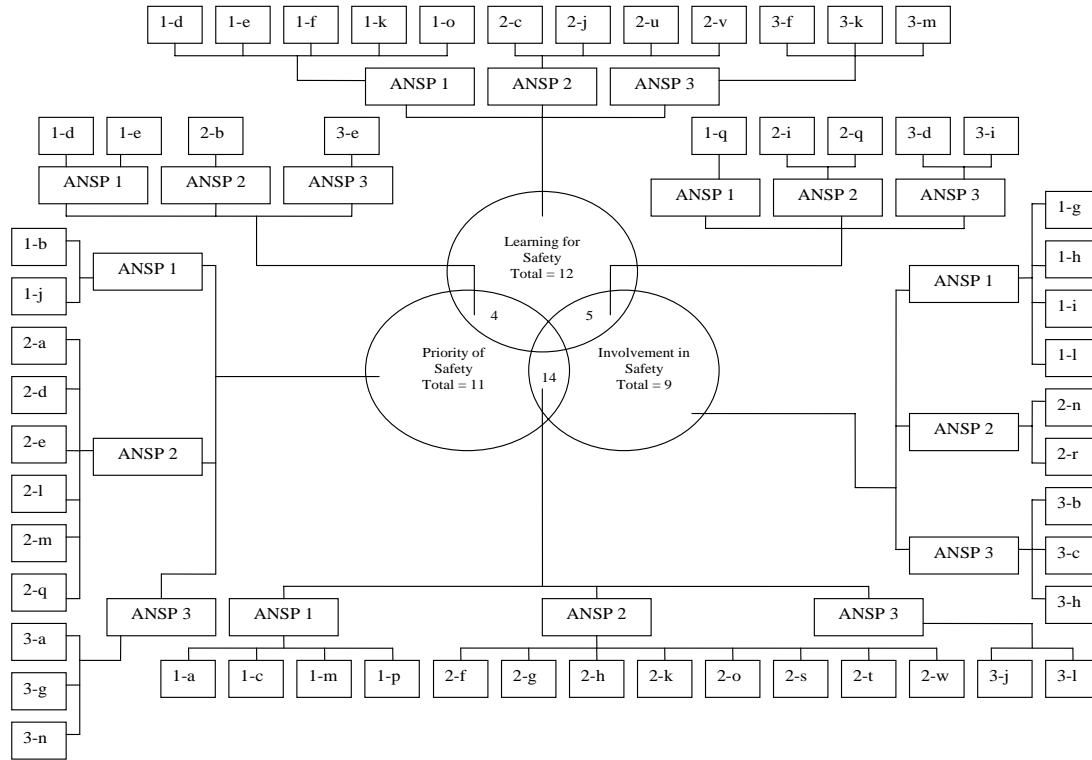
Figure 5: Summary of Safety Culture and Degraded Modes Observations in ANSPs from Phases 1, 2 and 3

Figure 5, summarizes the results from the three different phases of this study.   As mentioned, phase 1 studied ANSPs with significant over-flights but relatively limited regional operations. Phase 2 focused on ANSPs with high levels of over-flights and high volumes of domestic traffic.   Phase 3 looked at service providers with relatively low numbers of over-flights but with a significant volume of regional and domestic services.   The high-level overview in diagram 5 provides an indication of the relative importance of different components of a strong safety culture.   'Learning for Safety' and 'priority for safety' emerge as the two most significant areas. However, most concerns stem from the interaction between 'involvement in safety' and 'priority for safety'.   These results are indicative and tentative.   As mentioned previously, they are based on interviews, focus groups and work shadowing. The analysis may, therefore, be influenced by the subjective bias of the analysts.   However, the classification of each observation can be traced through figure 5 back to the previous sections of this paper so that interested readers can validate or refute the classifications presented in this summary.

The results of the high-level analysis in Figure 5 should not be surprising.   ANSPs must, typically, call upon support from a wide range of individuals and teams to address increasingly complex system failures. The use of sub-contractors is forcing ANSPs to broaden the scope of safety culture initiatives to ensure that suppliers have an equal involvement in safety.   There are also significant commercial and political pressures to meet levels of service in spite of problems in the underlying infrastructure. Concern to maintain levels of service to end users is increasing the need for regulatory support to ensure that safety

remains the priority in Air Traffic Management. Together these findings explain the relative importance of the interface between 'priority of safety' and 'involvement in safety'.

Rather than focusing on the distribution of safety culture topics across all three ANSPs, Figure 6 looks at findings that relate to 'learning for safety'. There is very little overlap between the issues raised during three phases of the project. This may suggest that there is little agreement over degraded modes and safety culture between the ANSPs with different traffic patterns. Alternatively, if more time had been available during the visits to each site then we might have identified common concerns in 'learning for safety'. Unfortunately, longitudinal studies were not possible given the numbers of service providers involved and the level of political/managerial support required for this initial comparative analysis.
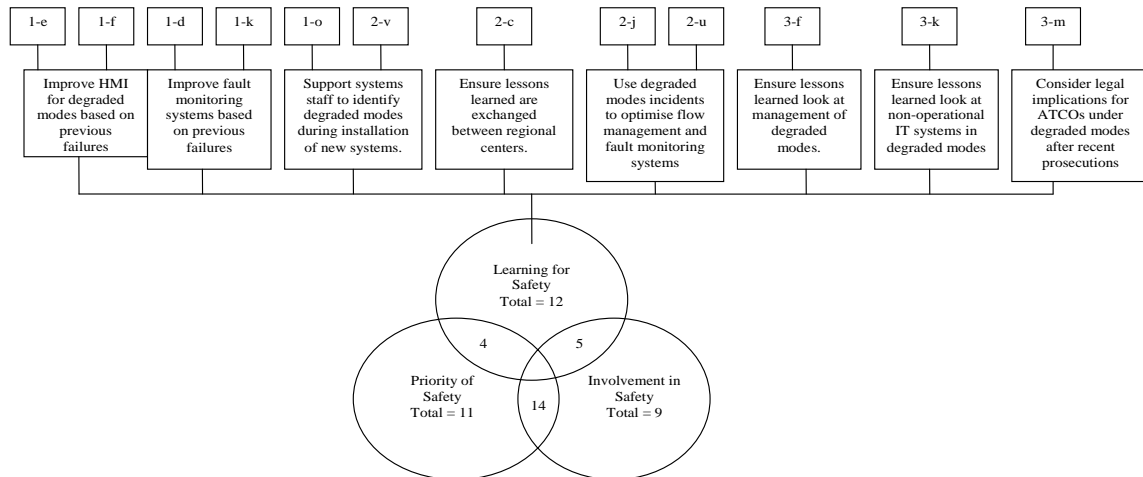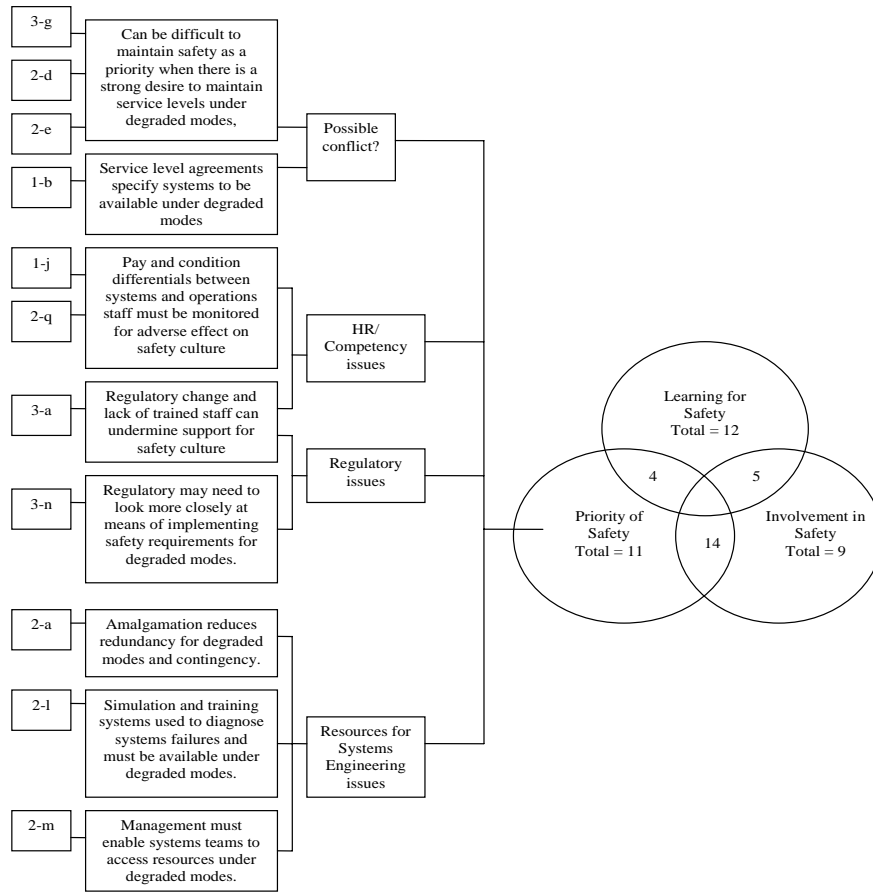

Figure 6: Summary of Safety Culture and Degraded Modes Observations on 'Learning for Safety'

Figure 6 also illustrates the range of concerns that were expressed about 'learning for safety' within the infrastructure providers during all three phases of the project. Some of the observations relate to improved fault monitoring and reporting systems to help staff to learn from past failures. Other observations deal with particular insights from previous incidents. For example, 3-m argues that there is a need to consider the impact of recent prosecutions following the Überlingen and Linate accidents. A third class of observations deals with more generic concerns. Several previous incidents described by the watches and by the systems staff during the visits were triggered or exacerbated by poor human-machine interfaces. Staff could not use their operational or engineering applications to identify and rectify the causes of infrastructure failures.

Figure 7 summarizes observations about the 'priority for safety' in ANSPs across all three phases of the project. Generic observations are grouped according to a number of common themes, including competency and human resource issues, regulatory concerns and issues to do with resources for systems engineering teams during degraded modes of operation. Even with this additional level of analysis, the concerns of the ANSPs seem to be remarkably different. For instance, the second group of ANSPs focused more on helping systems teams to combat degraded modes of operation, especially when key resources were shared with other operational or training teams. The third group of service providers was more concerned about the relationships between staff and regulators during infrastructure failures. However, all service providers share a common focus on human resource and competency issues. The focus and scope of these concerns differ, as can be seen in Figure 7.

Figure 7 also illustrates possible conflict between two observations made during different phases of the project. 1-b shows that service level agreements can specify those resources that are available to service providers during degraded modes of operation. However, observations 2-d and 3-g state that pressures to maintain particular levels of service may eventually these and other safety requirements. This example illustrates the need for additional work in this area. Further questions need to be raised about whether

service level agreements provide sufficient support during the longer-term and more immediate failures that characterize degraded modes of operation.

Figure 7: Summary of Safety Culture and Degraded Modes Observations on 'Priority of Safety'
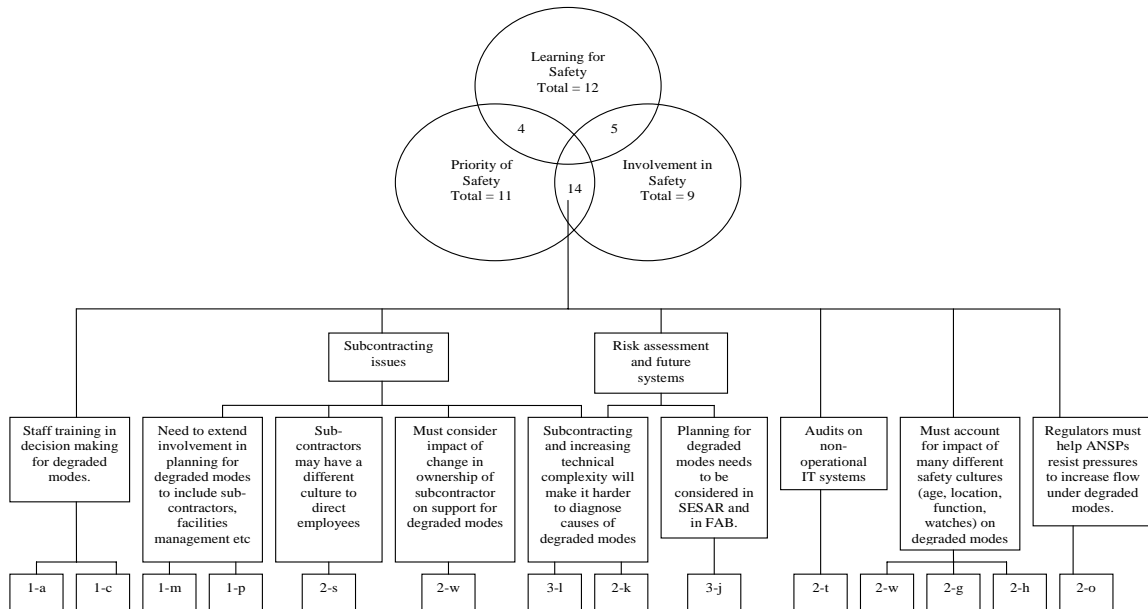
Figure 8: Observations intersection between 'Priority for Safety' and 'Involvement in Safety'

Figure 8 presents an overview of the observations that were made about the interface between 'involvement in safety' and 'priority of safety'. As can be seen, common concerns arose over the scope of any response to degraded modes of operation. The increasing use of sub-contracting proved to be an issue across all of the ANSPs. There was also a shared concern to ensure that the impact of degraded modes was considered within future systems for Air Traffic Management. Linate and Überlingen have illustrated the importance of the interaction between degraded modes and safety culture in previous accidents. These lessons should not be forgotten as we prepare for future systems to support FAB and Single European Sky ATM Research (SASAR).

Many people now recognize that organizational and cultural factors have a profound impact on safety management. However, the influence of safety culture on operational safety can seem obscure. By focusing on degraded modes, we have shown that the relationships between safety culture and operational safety are not vague and intangible; they are direct, immediate and complex. For the safety assessor who has to model system reliability, this paper provides a host of practical reasons why primary, secondary and fallback applications may not be sufficient to protect systems safety. For safety manages, as well as for regulators, there are many lessons that can be learned from the detailed insights into the tolerance towards degraded modes in air traffic operations. Safety culture may be seen as a 'soft' concept, but it often deals with hard issues.

References

J. Devine and A. Smith, Safety Culture Enhancement Activities and Next Steps within the Federal Aviation Administration, In Proc. of International Systems Safety Society, Baltimore, MD, August, 2007, ISSC, Unionville VA, USA, ISBN 0-9721385-7-9.

European Commission, Regulation No 549/2004 Of The European Parliament And Of The Council Of 10 March 2004 Laying Down The Framework For The Creation Of The Single European Sky, Official Journal Of The European Union, 2004.

European Commission, Regulation No 551/2004 Of The European Parliament And Of The Council Of 10 March 2004 On The Organisation And Use Of The Airspace In The Single European Sky, Official Journal Of The European Union, 2004a.

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 And C. Shea, A Comparison Of The Role Of Degraded Modes Of Operation In The Causes Of Accidents And Rail And Air Traffic Management. In Proceedings Of The 2nd IET Systems Safety Conference, The IET Savoy Place, London, ISBN 978-0-86341-863-1, 89-94, 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.