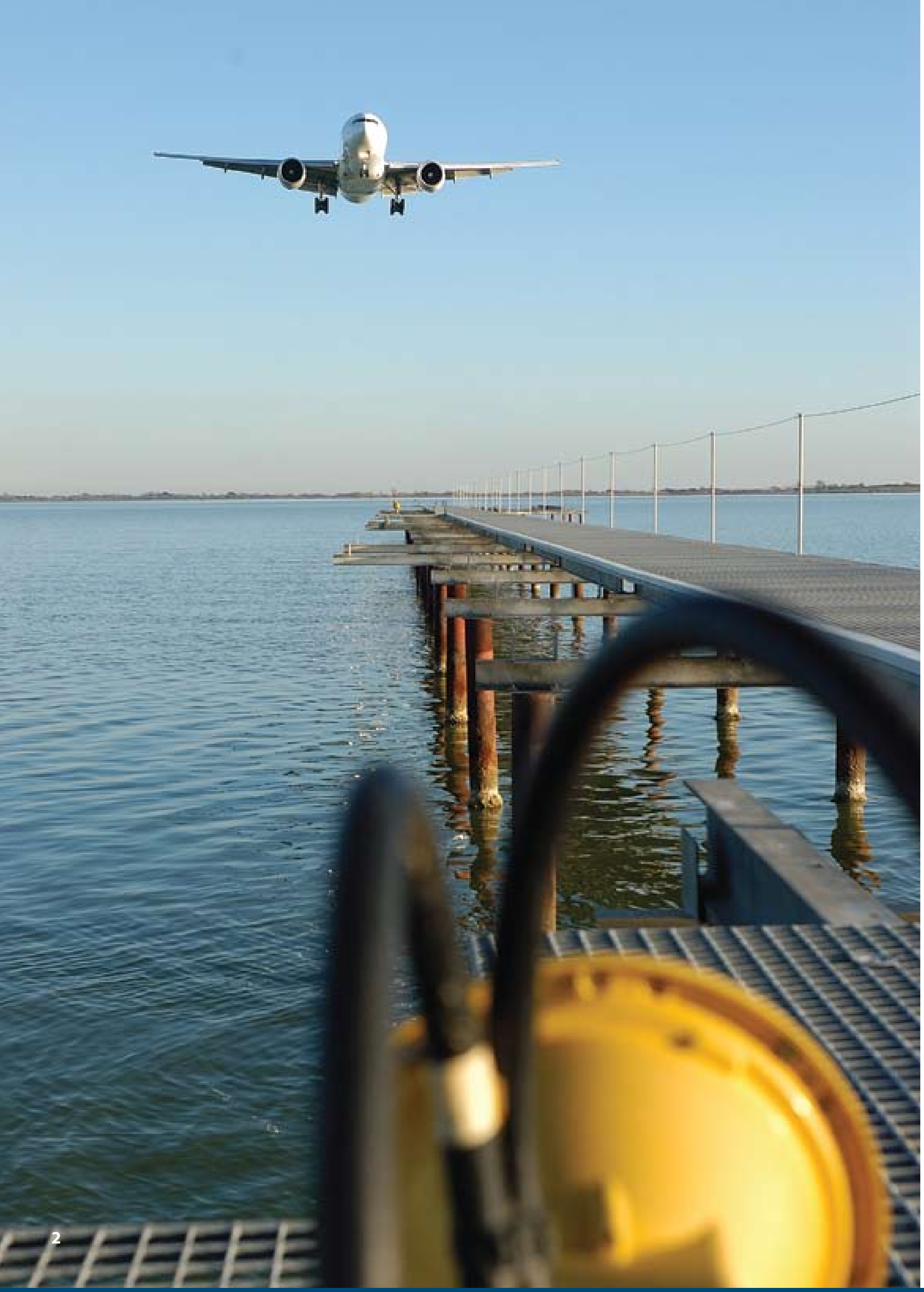
Degraded Modes Safety for Operational Engineering

ESP

Cooperative Network Design

October 2009

www.eurocontrol.int



INTRODUCTION

On the 8th October 2001 the Linate Airport disaster occurred killing 118 people. The airport had continued operations in thick fog, with limited surface movement radar, inappropriate runway markings and in multiple languages.

On the 1st July 2002 the Überlingen disaster killed 71 people. The disaster occurred during an FDPS update when telephone systems were unavailable, radio communications at the controller workstation were restricted, and a rostered controller was taking a break.

The two accidents represent degraded modes operations: i.e. controllers providing a service to aircraft when the "system" was not capable of supporting that service fully.

> *"The problem is that we get used to operating in degraded modes. Every day some system or another doesn't work, and we forget to question when it will be available or whether the data is accurate. As more services become unavailable, the result is that when a failure occurs, the ability to recover is practically nil".*
>
> *Professor Chris Johnson*
> *Chairman of the SESAR Scientific Committee*

Aimed primarily at the Engineering discipline, this brochure seeks to:

- Provide an overview of the degraded modes of operation
- Understand the relationship between safety culture and degraded modes
- Share the knowledge from an indepth 2008 ECAC study report
- Discuss tools for support in assessing degraded modes risk
- Provide resources for further information on degraded modes

WHAT ARE DEGRADED MODES OF OPERATION

It is best to think of degraded operations in the context of other modes:

Normal operations: are situations in which all elements of the system (including staff) are functioning as intended. Minor faults may need to be resolved, but they do not place restrictions on the systems and staff, and all routine tasks are achievable.

Degraded modes of operation: arise when problems in the underlying system occur. These are expected but are not considered normal. Staff have procedures for dealing with these situations and the risks associated with any failure are not considered significant. Reduced staffing levels are considered as an example of degraded modes.

Crisis: an adverse event that need not force a move from the operations room. More serious than degraded modes, they last for a shorter time than contingency, but may be severe in nature. Examples might include; strikes, floods & fires, security incidents, and bomb warnings.

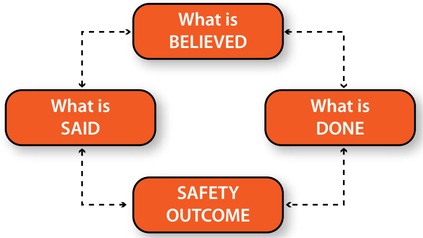
Contingency: represents a situation in which it is necessary to move from the standard operations room. These may be more long term than crises, and result in an interruption to the ATM service. Definitions and guidance may be found at **http://www.eurocontrol.int/ses/public/standard_page/sk_sesis_guidelines.html**

When we think of normal operations, degraded modes are becoming every day operations. We tolerate systems working imperfectly; we learn to ignore information that the system provides. This ”normal operation” contributed to the Linate disaster.

DEGRADED MODES AND SAFETY CULTURE

Safety Culture describes the realities of safety: the way that safety is done, not necessarily the way that people say it is done. The way we think about safety affects our behaviours and what is done. The way we speak about safety affects what is believed. All of these affect safety outcomes in our daily working lives.

"The way that safety is done around here".



Safety Culture

No ANSP will say that it does not take safety seriously, and rightly so. However, we need to scrutinise safety and ask what safety actually looks like on the ground:

- Is the operations room running with too few controllers?
- Are multiple systems unavailable as a result of maintenance?
- Are Engineers short staffed and working extra shifts?
- Have equipment upgrades been postponed due to other funding priorities?
- Is there a clash between terminal facilities investment and runway infrastructure investment?
- Who owns the network switch that handles your data?

At what point does a normal operation become a degraded mode?

By tolerating degraded modes we are reducing our commitment to safety.

THE INCIDENT PIT

When an insect lands on a "pitcher plant" it is attracted to the nectar in its deep neck. As the insect moves from the top over the crest of the flower it falls; it has passed a point from which it cannot escape. The sides of the plant are too slippery and steep for it to escape. The insect drowns.

The pitcher plant analogy, when applied to degraded mode operations, is what we call the "incident pit".

The incident pit leads us into unrecoverable situations in similar ways. There are factors which push us into the incident pit. Each represents a set of management, operational and engineering decisions made before or in response to an event. Eventually a point is reached where it is inevitable that an incident will occur: at that point we fall to the bottom of the pit.

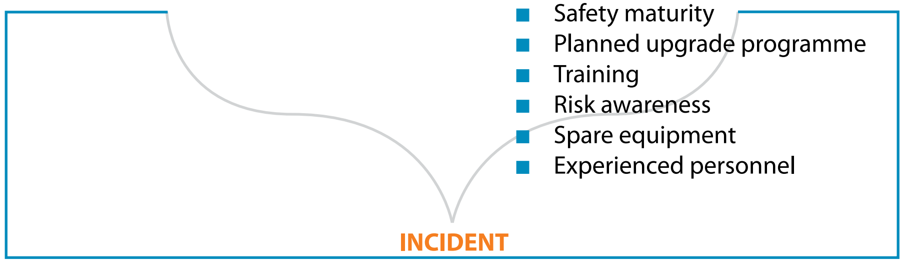
There are a similar set of barriers that keep us out of the pit: best practice, safety maturity, infrastructure investment etc. The systematic removal and degradation of these barriers occurs during degraded modes of operation.

Pushing us into the pit

- Staff shortages
- Limited secondary systems
- Limited experienced resources
- Legacy equipment
- 3rd party systems, support contracts
- Intermittent failures
- Concurrent breakdowns

Keeping us out of the pit

- Risk assessment
- Contingency plans
- Spare personnel
- Fully functioning equipment
- Incident investigation & learning
- Safety maturity
- Planned upgrade programme
- Training
- Risk awareness
- Spare equipment
- Experienced personnel



The Incident Pit

DEGRADED MODES & MAJOR INCIDENTS

Two major accidents are described below, and for each the degraded mode is clarified. Have you learned the lessons from each of the incident reports?

Could these incidents happen at your unit?

Linate

In poor visibility, a Cessna crossed the runway threshold and was struck by an MD80. The MD80 crashed into a baggage hall and 118 people were killed. Beyond pilots and controllers, the whole ATM operation was severely degraded:

- Runway maps did not represent actual runway markings
- Surface radar ineffective
- Runway lighting ineffective
- Stop bars ineffective
- Another incursion 24h earlier

Why did operations continue?

Überlingen

A Tupolev and Boeing collided in mid air killing 71 people. Confusion over TCAS alerts was identified as the primary reason for the accident, but degraded modes also played a significant role:

- FDPS update in progress
- RVSM being introduced
- Phone lines ineffective
- RT frequencies not on same workstation
- STCA audible only
- Similar incidents occur often

Why did operations continue?

Many of the above items are common across ANSPs.

How robust is your system?

In response to such events, what should your organisation do?

AIRCRAFT, EQUIPMENT PROVIDERS AND ANSPs

On behalf of EUROCONTROL, Professor Chris Johnson reviewed the activities of system manufacturers, ANSPs and aircraft manufacturers in order to determine the industries' appreciation of degraded modes. The combined picture of all services is necessary to constitute a fuller understanding of degraded modes in the aviation industry, not just ATM, and where sources of degraded modes might arise. Not all the observations were negative.

Aircraft manufacturer's view

- Airlines continue to rely on fallible components even when they have been implicated in incidents.
- Design flaws are exacerbated by maintenance procedures 3rd party servicing.
- Solving technical degraded mode issues may be possible, but those related to "soft issues", i.e. people, are difficult for technical organisations.
- Masking faults in "tolerant" systems removes the crew from a clear picture of aircraft faults.
- It is not always possible to predict all degraded modes.
- The provision of redundancy does not necessarily avoid the issues related to degraded modes.
- Commitment to product extends to the life of the product - **positive**
- Local 3rd party maintenance organisations will feed back to a manufacturer to educate them on maintenance of their product - **positive**

Equipment manufacturer's view

- The need to work within budgets and timescale will lead to shortcuts embedded within equipment.
- Equipment support contracts do not cover 3rd party equipment within the total system.
- Systems may shed more advanced features if they are struggling with data volumes.
- Specialised equipment for ACCs will not provide the same level of support for units that are not ACCs. Similarly specialised aiport and terminal control systems will not support ACCs effectively.
- Project teams in whom customers have trust will be disbanded following delivery to the client.
- The customer's process of commissioning should address degraded modes and identify which systems may fail and who is responsible for them.
- Technical supplier and operational views of the same issues will be significantly different.
- The understanding of safety for manufacturers is very different to that of the ANSP.
- If subcontracting for a larger supplier, engineers have no opportunity to express concerns about the larger product.

ANSPs' view

Findings from visits across European ANSPs highlighted common observations. These are detailed below. How does you ANSP address the questions they raise?

- Can you distinguish between systems that are redundant and those that are fall-back. Are fall-back systems used for periods of degraded mode operations?
- Self-healing and redundant systems mask true fault conditions. What maintenance is necessary for redundant systems?
- Sales, maintenance and support contracts can be unenforceable when equipment actually fails – what service do you anticipate, what will you receive?
- Is it clear to controllers when a system is operating without redundancy or in fall-back mode?
- Rectifying degraded modes introduces new hazards, how are these identified and dealt with?
- Advanced technical systems used in ATM require sub-systems to create interfaces for the equipment to work seamlessly. How have these been built? Does your ANSP rely on a 50€ network card?
- Do your subcontractors have the same attitude to safety as your staff?
- Are engineering training facilities of a similar standard to controller training facilities?
- How dependent on neighbouring states are you for primary systems?
- What is the knock-on effect to other ANSPs of a failure in one of your Units?
- Where is the safety department when trying to resolve a degraded mode?
- Who is responsible for imposing and lifting flow restrictions during degraded modes; what pressures are put on operations and engineering and by who?
- How do you contact emergency decision-makers when required? Does it work?

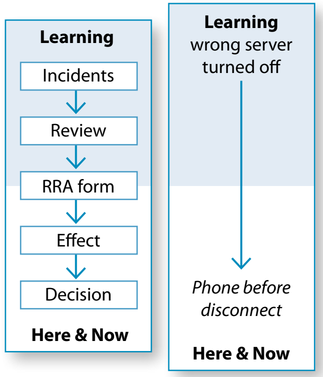
"The more progressive companies visited implemented a form of rapid risk assessment before beginning resolution actions"

- Freezing equipment budgets during procurement or limiting functionality results in shortcuts or reduced service. How is this managed?
- The more progressive companies visited implemented a form of rapid risk assessment before beginning resolution actions.
- Do ACCs and Towers (TC) manage systems in the same way across the organisation; do "they" take risks that you don't?
- How well equipped are the "regions" to deal with degraded modes, what support do they have ?
- What documentation do you rely on, maps, plans etc. that are not maintained because they are not "safety documentation"?
- What risk assessment is made before putting hands on a piece of equipment and changing its status?
- Could an engineer be prosecuted in the event of a passenger fatality caused by your ANSP?

RAPID RISK ASSESSMENT

How often do we review risks for existing equipment? How often do we assess risks before making a decision on the actions needed to resolve an incident? Rapid Risk Assessment (RRA) is a tool for structured assessment of situations that would not normally be assessed.

RRA is used in the defence industry to assess key operational decisions that will expose troops and equipment to risk. This may be enemy fire or routine operational decisions about equipment movement. In each case, troops on the ground are now trained in assessing and implementing RRA to aid decision-making in critical situations.



Learning

Incidents → Review → RRA form → Effect → Decision

Here & Now

Learning
wrong server turned off

Phone before disconnect

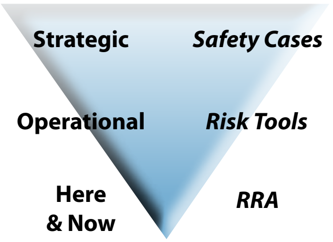
Here & Now

RRA in context

The RRA approach uses lessons learned and provides an assessment of the major contributors to previous accidents and incidents.

The RRA assessment form is a "living" document and is regularly reviewed in light of new incidents.

Where decisions that might have an impact on operations and safety have to be made quickly, a RRA tool provides an on-the-ground aid for Engineers. Based on the incidents in your unit, a RRA tool can bring learning from past events to the here-and-now in moments. What RRA tool do you use?



Strategic — ***Safety Cases***

Operational — ***Risk Tools***

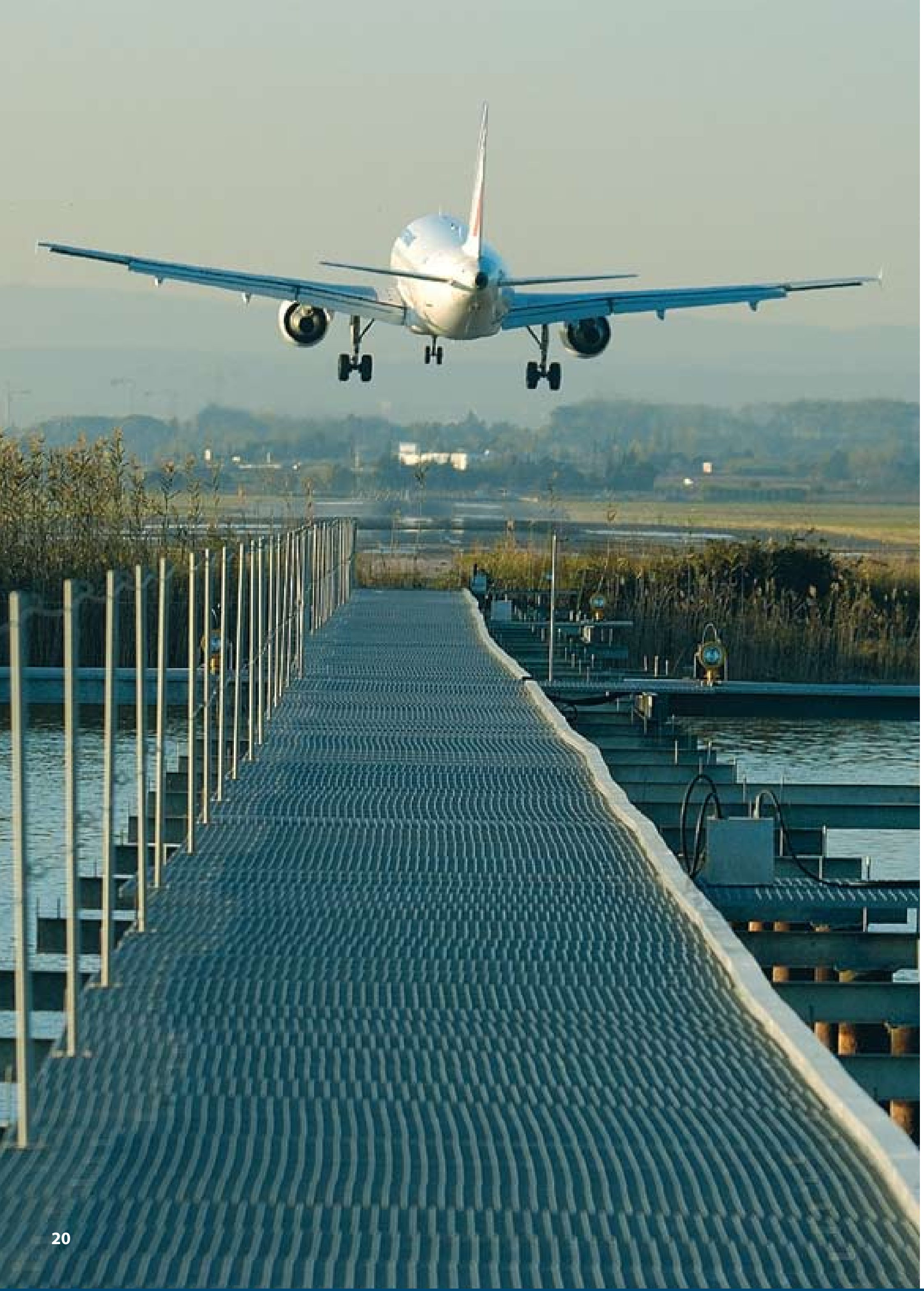
Here & Now — ***RRA***

- **Changes over time**
- **Changes with equipment**
- **Changes with staff & management**

How does this happen in your organisation?

"If the primary fails, the back-up will not be able to handle the traffic; but it isn't safety critical because it's back-up, so we don't have to do a safety assessment for it"

Unnamed ANSP 2008 - Europe



DEGRADED MODES CHECKLIST

When we look at incidents and accidents with perfect hindsight it is clear where the problems in organisations lie. But do we ask these questions on a daily basis, and do we ask them before acting – preventing an incident from becoming an accident? A hardy mnemonic for deciding if it is safe to proceed is given below:

P	**P**aths leading to failure understood
A	**A**ssess risks before action taken
R	**R**ecovery paths understood
I	**I**nformed all points of communication
S	**S**econdary systems available and unaffected

A QUESTIONING CULTURE?

No ANSP would admit that safety does not have top priority, but when we think of safety we need to broaden the definition to include safety culture, and consider how we think, act and learn in relation to safety. How an ANSP deals with, and how its engineers think about, degraded modes directly influence safety and how we learn from our own and other ANSPs' degraded modes experience.

- Where is responsibility and liability in management and service contracts?
- What are the single point failures in your systems?
- Can you communicate, and do back-up communication systems actually work?
- Have you assessed flooding and water ingress sources including fire fighting?
- Do new systems require you to update detailed fire safety assessments?
- Do you understand the hardware in your servers and telecoms infrastructure?
- Where is your infrastructure degrading; what happens if it fails tomorrow?
- Where have you introduced vulnerabilities into your facilities management?
- Will fall-back modes really work, have you tested them?
- Are fall-back systems safety critical systems or just back-ups?
- Do you understand the risk of removing a network card from a multiplexer?

Risk is continually on the move – do you understand your risks?
Do you have a safe culture?

FOR FURTHER INFORMATION CONTACT:

EUROCONTROL is developing a training course for ATM Engineers on degraded modes safety, including awareness of Rapid Risk Assessment. For more information contact one of the people below.

Chris Johnson

is a professor at Glasgow University and has worked with EUROCONTROL for the past 14 years in the field of incident investigation and safety. It is Chris's work that has been the major contributor to the production of this brochure. Chris has recently been appointed to the SESAR Scientific Committee.

johnson@dcs.gla.ac.uk

Barry Kirwan

is safety research leader at EUROCONTROL, researching, developing and implementing new safety approaches, supporting incident investigations at Maastricht, co-chairing the FAA-EUROCONTROL Action Plan on Safety Research, and leads the European Safety Culture programme.

Barry.kirwan@eurocontrol.int

Andy Kilner

has spent 17 years working in human centred processes and safety including ATM, conventional defence, civil nuclear & electronics. He now works at EUROCONTROL as a safety expert and is contributing to research in the fields of degraded modes, human reliability analysis, safety culture and the wider SESAR project.

Andrew.kilner@eurocontrol.int

Tony Licu

has a background as a controller and engineer. He has managed EUROCONTROL's Strategic Safety Action Plan and European Safety Programme for ATM (ESP) implementation, and Just Culture with the aim of clarifying and promoting the concept. Tony leads the Safety KPI development work in Europe and manages the Network Development Pillar of safety and human factors, within EUROCONTROL.

Antonio.licu@eurocontol.int