EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

This Document is issued as EATM Reference Material. The contents are not mandatory. They provide information and explanations or may indicate best practice.

Managing System Disturbances in ATM: Background and Contextual Framework

Edition Number	**:**	**1.0**
Edition Date	**:**	**31.08.2004**
Status	**:**	**Released Issue**
Intended for	**:**	**EATM Stakeholders**

DOCUMENT CHARACTERISTICS

TITLE		
Managing System Disturbances in ATM: Background and Contextual Framework		
	EATM Infocentre Reference:	040201-13
Document Identifier	**Edition Number:**	1.0
HRS/HSP-005-REP-06	**Edition Date:**	31.08.2004

Abstract

System disturbances are likely to be a key factor affecting the acceptance and safety of future automation. Neither hardware nor software can be claimed to be totally reliable and so humans are always required in Air Traffic Management (ATM) systems, which will remain *socio-technical* systems. Unfortunately, human reliability is also fallible. Hence, an understanding of how humans manage system disturbances is required, along with a method for looking at the problem for new systems.

This report details research and operational experience regarding the management of system disturbances. Findings from the literature (both ATM and non-ATM) are contextualised by interviews with thirty ATM personnel in three European Air Traffic Control (ATC) centres. This background information is structured around a contextual framework, which itself is the basis for a tool for analysing how humans are likely to recover from functional disturbances, called the Recovery from Automation Failure Tool (RAFT).

This document has been produced as part of the 'Solutions for the Human-Automation Partnerships in European ATM (SHAPE)' Project managed by the Human Factors Management Business Division (DAS/HUM) of EUROCONTROL.

Keywords

Automation	Computer Support	Cognitive Support	ATM System	Failure
Disturbance	Malfunction	Human Recovery	Detection	Diagnosis
Correction	Monitoring	Control	Engineering	

Contact Persons	Tel	Unit
Oliver STRAETER	+32-2-729 5054	Safety and Security Management Business Division (DAS/SSM)
Manfred BARBARINO	+32-2-729 3951	Human Factors Management Business Division (DAS/HUM)

Authors

S. Shorrock and O. Straeter

STATUS, AUDIENCE AND ACCESSIBILITY

Status		Intended for		Accessible via	
Working Draft	☐	General Public	☐	Intranet	☐
Draft	☐	EATM Stakeholders	☑	Extranet	☐
Proposed Issue	☐	Restricted Audience	☐	Internet (www.eurocontrol.int)	☑
Released Issue	☑	*Printed & electronic copies of the document can be obtained from the EATM Infocentre (see page iii)*			

ELECTRONIC SOURCE

Path:	G:\Deliverables\HUM Deliverable pdf Library\	
Host System	**Software**	**Size**
Windows_NT	Microsoft Word 8.0b	

EATM Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: eatm.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
SHAPE Project Leader	O. STRAETER	12.07.2004
Chairman HRT Human Factors Focus Group (HFFG)	V.S.M. WOLDRING	12.07.04
Manager EATM Human Resources Programme (HRS-PM)	M. BARBARINO	13.07.2004
Chairman EATM Human Resources Team / Programme Steering Group (HRT/PSG)	A. SKONIEZKI	19.07.04
Director ATM Programmes (DAP)	G. PAULSON	27.7.04

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	30.06.2003		Working Draft	All
0.2	26.08.2003		Draft	All
0.3	17.12.2003		Proposed Issue for HRS-PSG Meeting in January 2004 (document configuration and editorial changes)	All
1.0	31.08.2004	040201-13	Released Issue (agreed on 28-29.01.2004) (final document configuration and editorial adjustments)	All

CONTENTS

Page intentionally left blank

EXECUTIVE SUMMARY

Automation is the partial or full performance by a machine system (mechanical or electronic, or both) of a function previously performed by a human, or which conceivably could be performed by a human. Automation has been developed for decades, though most existing technology is now seen simply as machine operation. Automation is necessary to increase capacity and to improve or maintain safety. Some of the justifications for automation include reliability, speed and (processing) power. However, no automated function is totally reliable, and even if functions are 'reliable' they may behave in unexpected ways due to unforeseen interactions between system components. So, assuming that an automated function will fail sooner or later and that any backup system will, by the same token, also display this tendency, it becomes obvious that humans are required in some role as part of the socio-technical system. This role normally includes a monitoring and backup role. With increasing automation, the human role – unless very well planned and designed – naturally becomes increasingly reactive and passive, and the human is increasingly distanced from the process itself. But humans are also fallible and, paradoxically, tend to become more unreliable in this 'out-of-the-loop' role when automation is more reliable. At the same time, the processing speed and power of automation – two of the key automation justifications – coupled with increased technical system complexity and traffic density, diminishes the time available to deal with disturbances. Such issues point to a pressing need to understand how people manage system disturbances.

This report utilises a contextual framework, constructed from research findings and operational experience, to help guide a discussion of the process by which people recover from system disturbances. The framework describes the context and cause of a problem, the problem itself, the effect and exposure, the recovery process, and the outcome. The report details research and operational experience regarding the management of system disturbances. Findings from the literature (both ATM and non-ATM) are contextualised by interviews with thirty ATM personnel in four European ATC centres.

The framework, along with the research findings and operational experience, is also the basis for a tool called the '**Recovery from Automation Failure Tool' (RAFT)**'. RAFT is a method for analysing functional disturbances and helps to consider systematically the concepts within the RAFT Framework. RAFT is available separately in electronic form. It is proposed that RAFT provides an appropriate predictive method for examining system disturbances in ATM, which can be verified using measures of recovery performance in simulated or operational environments. Further work is recommended to apply, test and refine the approach, and to develop companion 'RAFT principles' to help system designers to design ATM systems with recovery 'built-in'.

Page intentionally left blank

1. INTRODUCTION

1.1 Background

The work on management of system disturbances in ATM presented here is embedded in a larger project called 'Solutions for Human-Automation Partnerships in European ATM (SHAPE)'. The SHAPE Project started in 2000 within the Human Factors Sub-Programme (HSP) of the EATMP Human Resources Programme (HRS) (see EATMP, 2000) conducted by the Human Factors and Manpower Unit (DIS/HUM) of EUROCONTROL, today known as 'Human Factors Management Business Division (DAS/HUM)'.

SHAPE is dealing with a range of issues raised by the increasing automation in European ATM. Automation can bring success or failure, depending on whether it suits the controller. Experience in the introduction of automation into cockpits has shown that, if human factors are not properly considered, 'automation-assisted accidents' may be the end result.

Seven main interacting factors have been identified in SHAPE that need to be addressed in order to ensure harmonisation between automated support and the controller:

- Trust: The use of automated tools will depend on the controllers' trust. Trust is a result of many factors such as reliability of the system and transparency of the functions. Neither mistrust nor complacency are desirable. Within SHAPE guidelines were developed to maintain a correctly calibrated level of trust (see EATM, 2003a, b, c).

- Situation Awareness (SA): Automation is likely to have an impact on controllers SA. SHAPE developed a method to measure SA in order to ensure that new systems do not distract controllers' situation awareness of traffic too much (see EATM, 2003d).

- Teams: Team tasks and performance will change when automated technologies are introduced (team structure and composition change, team roles are redefined, interaction and communication patterns are altered). SHAPE has developed a tool to investigate the impact of automation on the overall team performance with a new (see EATM, 2004a).

- Skill set requirements: Automation can lead to both skill degradation and the need for new skills. SHAPE identifies new training needs, obsolete skills, and potential for skill degradation aiming at successful transition training and design support (see EATM, 2004b).

- Recovery from system failure: There is a need to consider how the controller will ensure safe recovery should system failures occur within an

automated system (covered by this report). A successful recovery from system failure needs proper managing system disturbances.

- Workload: With automation human performance shifts from a physical activity to a more cognitive and perceptual activity. SHAPE is developing a measure for mental workload, in order to define whether the induced workload exceeds the overall level of workload a controller can deal with effectively (see EATM, 2004c).

- Ageing: The age of controllers is likely to be a factor affecting the successful implementation of automation. Within SHAPE this particular factor of human performance and its influence on controllers' performance, are investigated. The purpose of such an investigation is to use the results of it as the basis for the development of tools and guidance for supporting older controllers in successfully doing their job in new automated systems (see EATM, 2003e). An additional report provides a questionnaire-survey throughout the Member States of EUROCONTROL (see EATM, 2004d).

These measures and methods of SHAPE support the design of new automated systems in ATM and the definition of training needs. It also facilitates the preparation of experimental settings regarding important aspects of human performance such as potential for error recoveries or impacts of human performance on the ATM capacity.

The methods and tools developed in SHAPE will be compiled in a framework in order to assist the user in assessing or evaluating the impact of new systems on the controller performance, efficiency and safety. This framework will be realised as a computerised toolkit called the 'SHAPE Toolkit' and is planned to be available in 2004.

1.2 Automation: Description and Justification

Automation is the partial or full performance by a machine system (mechanical or electronic, or both) of a function previously performed by a human, or which conceivably could be performed by a human. The development of technical automation capabilities has been rapid and opportunities for its implementation widespread. Machines, particularly computers, are now capable of performing not only many functions which previously only humans could perform but also many functions which humans could perform but not very well. The identification of an automated function is not always clear-cut. Parasuraman *et al*. (2000) argue that the replacement of electrical cables with fibre optics, or the upgrading of a computer, probably does not constitute automation. However, if a new technology performs a function that was never performed by a human and probably could never be performed by a human, then this does not constitute automation either. Another issue is that what is conceived as automation now will not necessarily be considered to be automation in the future. Instead, it will simply be seen as *machine operation*. Take for example the everyday simple example of the mechanical clock or watch, which automated a 'manual' method of determining the approximate

time, for instance by using sun-dials. Now the clock is seen as a simple machine. The introduction of digital clocks and watches did not represent automation, but rather a change in the way that an already automated function was carried out.

Automation in ATM is developing at a faster rate than ever before. ATM automation has, in the past, been concerned with information integration, such as secondary radar and electronic flight strips. It is anticipated that future forms of ATM automation will reach higher levels of information processing and play a more active role in prediction, problem solving, decision-making, task sequencing and task scheduling, with the result that the controller role is likely to change to become that of a traffic manager and potentially in future, that of a system supervisor.

The impetus for the implementation of automation is usually to improve productivity, increase capacity and maintain or improve safety. To achieve these functions, it is assumed that a particular machine (hardware and software) performs a function to higher standards than can be, or generally are, achieved by human. The criteria may include, for instance, speed, accuracy and reliability, power, and cost. Automation clearly performs many functions far more quickly than humans, such as mathematical calculations and component assembly. Accuracy is also often improved with automation, for instance with the two previous examples, and for other activities, particularly where both speed and accuracy are required. Another key justification for automation is to reduce or eliminate human error. However, the issue of human error is now known to be far more complex than this. Human reliability varies under various conditions, such as fatigue, stress, task load and ambient environment. Some of these conditions may remain fairly constant (task design, for instance). Other conditions will vary over time (fatigue being a good example), and human reliability will reduce whereas automation reliability will not (though in the much longer term mechanical equipment will, but in more predictable ways). Also, machines can provide power or force beyond human capabilities, taking for instance the electric drill or jack-hammer, both of which replaced manual alternatives. Cost is a major justification, of course – humans are a considerable long-term cost, while automation (particularly software) represents a major capital expenditure, but will usually pay for itself in a relatively short period.

Automation is seen as a necessary and inevitable development for ATM, justified on the grounds of speed, accuracy and reliability, power, and cost. However, some of these justifications are not so straightforward.

1.3 Automation Reliability

While the potential benefits of automation cannot be disputed, especially economic benefits, trade-offs and problems resulting from the use of automation exist. Two classes of problems have been suggested in the literature (Parasuraman and Riley, 1997; Wickens *et al*., 1997; Woods, 1993,

1996). Some problems may be the result of how the automation is implemented in practice. These are generally less serious and can be resolved by adequate, well-planned and structured training. The other class of more insidious problems may arise from unanticipated interactions between the components[1] of the work-system in which the automated system is implemented.

Reliability merits further consideration in the context of this work. Reliability is the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions (Leveson, 1995). *Software reliability* is slightly different in that software does not fail in the way that mechanical components fail (software does not 'wear out') but it does exhibit erroneous behaviour due to design errors. Software reliability is therefore defined as compliance with the requirements specification (Leveson, 1995).

Reliability and safety are overlapping, but not identical concepts. Safety is a much broader term and is an *emergent system property*. Safety is concerned with more than just failures; failures may occur without resulting in an accident and accidents may occur without any component failure. Hence, it is important to understand several caveats relating to reliability:

- First, a system may have high reliability but still lead to accidents. Equipment may function outside the parameters and time limits specified in the reliability equation, or software may function exactly as specified in the requirements specification (i.e. correct and totally reliable), but still lead to accidents.

- Second, events leading to an accident will normally be a complex combination of factors, which may include design errors, equipment failure, poor maintenance, human operating error, etc. Indeed, components may work as intended individually, but together bring the system into a hazardous state. The complexity of hardware and software may preclude testing for all possible failures and faults, particularly where these stem from interactions between sub-systems.

- Third, generalised reliability probabilities may not hold true in certain specific cases or areas. Reliability engineering requires certain assumptions about the operational environment, and not all of these may be foreseeable.

- Fourth, reliability data often represent an average or mean (e.g. mean time to failure), rather than the variance around the mean. Hence, such average figures can be deceiving.

Accepting the above, it is also clear that unreliability can negatively affect safety and human performance. Very rarely, if ever, can equipment or

[1] The components of the work system consist of the human operator, the automated system and any other system in the workplace.

software be guaranteed to be 100% reliable. Automation will exhibit various disturbances, from spurious or erroneous output to total loss of function, associated with failed physical components and erroneous software.

Reliability and safety are overlapping, but not identical concepts. Equipment or software is rarely, if ever, totally reliable. Unreliable system components can negatively affect safety and human performance, but reliable system components will not necessarily result in a safe system.

1.4 Human Roles and Automated Systems

Automation rarely, if ever, eliminates the human from the system. First of all, humans are required to design the systems in the first place. This is a significant, perhaps the most significant, source of errors. Errors can be made in the requirements, the specifications and the coding of software. Humans are also required to manage and maintain systems, overseeing system changes, upgrade, maintenance, cleaning, etc. Again, errors can occur here, all of which can conceivably contribute to an accident.

Even where humans are removed from the immediate control activities, people are still necessary to monitor that the system is working as intended. Sheridan (1980) stated that automated systems change the role of the operator from a controller to a supervisor. There are many potential counter-arguments, but each of these proves difficult to sustain on closer analysis. For instance, one can argue for high levels of redundancy in a system; deliberate duplication to improve reliability. Equipment may be redundant, for instance through use of standby spares or concurrent use of multiple devices to perform a function with ‘majority voting’ on the results. Redundant software may also be designed, with multiple versions available to perform the same function. However, redundant systems can be affected by *common cause failures* (such as a failure of common power supply, or erroneous software specifications), or *common mode failures*, where multiple components fail in the same way (for instance to due design or maintenance errors).

Another logical counter-argument to the need for human monitoring is to use an independent machine to monitor the automation. Norman (1990) states that to build an automated system with a self-monitoring capability that would allow it to recognise that conditions are changing would require a higher-level of awareness – monitoring of its own monitoring abilities. According to Leveson (1995), this is currently unachievable in a general sense. The question arises as to who, or what, monitors the monitoring system. For a human to attempt this task simply removes the human even further away from the process. Endsley and Smolensky (1998) state that controllers will need situation awareness (SA) even under conditions of full automation to: a) monitor the automated system and to integrate the outputs of an automated system with other tasks; and, b) detect system disturbances and to intervene effectively.

Redundancy and machine monitoring jointly produce another problem by increasing the level of system complexity. Perrow (1984) argues that accidents are a ‘normal’ and expected outcome of complexity and tight coupling in a high-hazard environment.

A second important human role, as indicated by Endsley and Smolensky (1998), is that of backup. So, when a safety-critical function (e.g. conflict detection) fails, either due to a single failure/error or a combination of failures/errors, then the human is required to a) continue to perform the function and b) correct and reinstate the failed equipment or erroneous software (since operational capacity may depend on the automated performance of the function). It can be seen, then, that the human’s role in automated systems shifts from active control to ‘supervisory control’, in particular, detecting and correcting problems. Hence, in light of the various human roles that are required even with highly automated systems, one of the key justifications for automation is questionable – that of removing human error and hence improving system reliability. Table 1 describes some of the problems associated with the roles of 'human as monitor; and ’human as backup’ (summarised from Leveson, 1995).

Table 1: Two problematic roles for the human in automated systems (after Leveson, 1995)

Role	Problem
Human as monitor	*1. The task may be impossible* Automatic control systems are used to replace humans because they can do the job more quickly or effectively than humans, but then humans are required to monitor in real time that the automatic system is performing effectively.
	2. The operator is dependent on the information provided; it is easy to provide too much or too little information or to display it poorly Computers often overload operators with too much or too complex information. Otherwise, operators may have to manipulate the system in unexpected ways to figure out how it works.
	3. The information is more indirect with automated systems, which may make it harder for the operator to obtain a clear picture of the state of the system Automation removes operators from the system; the relationship between actions and outputs is indirect and abstract. Thus, it is difficult to form an appropriate mental model of the system, which may be needed to assist decision-making about unexpected events.
	4. Failures may be silent or masked Disturbances may be masked or delayed in their early stages by system behaviour that is designed to cope with such deviations, attempting to maintain a constant system state.
	5. *Tasks that require little active operator behaviour may result in lowered alertness and vigilance and can lead to complacency and over-reliance on automated systems* Even highly motivated individuals find it impossible to maintain effective visual attention for rare events such as abnormalities. Ironically, highly reliable automated systems increase complacency and unreliable systems reduce complacency.
Human as backup	*1. A poorly designed human-machine interface may leave operators with lowered proficiency and increased reluctance to intervene* People in control need both manual and cognitive skills, but both skills deteriorate when they are not used, so that experienced operators have inaccurate mental models and behave more like inexperienced operators. Lack of control experience or declining skills may result in a reluctance to intervene.
	2. Fault-intolerant systems may lead to even larger errors Systems may fail in ways that designers did not anticipate, and yet designers may be so sure that their systems are self-regulating that they do not include appropriate means for human intervention.
	3. The design of the automated system may make the system harder to manage during a crisis Automated systems may require that operators jump back in the loop from 'cold', switching quickly from a passive monitoring role to an active emergency handling role, making many decisions under time pressure with an inadequate mental model of 'picture'.

Humans are still essential when automated systems are introduced. Two key roles include monitoring and backup, roles that are required regardless of the layers of built-in redundancy and machine monitoring. The result is that people take on a more passive and reactive role, which can be problematic.

1.5 System Control: A Critical Partner in Managing System Disturbances

Air traffic control personnel already monitor a number of aspects of system reliability relating to data quality. Examples of such activities include 'passive' checking (i.e. detecting anomalies) of the quality and integrity of code-callsign conversion, Mode C (e.g. intermittent), and radar coverage, checking the proper functioning of input devices, displays, etc. However, this form of monitoring is limited to a number of functions as they directly affect the controller. Behind the scenes, *system control* personnel provide a critical partner in maintaining Air Traffic Management / Communication, Navigation and Surveillance (ATM/CNS) systems. System control personnel monitor and control all of the equipment that supports the controller, reconfigure and maintain degraded or failed equipment with minimum disruption of the controller's tasks, and provide a direct communication link with ATC, that is they inform controllers of the status and performance of equipment and systems, and receive reports of technical problems. Managing system disturbances is a cooperative endeavour.

New technology is becoming more software-intensive and distributed network-oriented, with the relatively new addition of space-based systems. Wickens *et al*. (1997) note that new technology is moving toward automation of control and monitoring functions such as:

- data sensing, searching, acquisition and storage;
- calculation;
- diagnostics and fault localisation for modularised equipment;
- reconfiguration and automated switching to redundant backup components or software versions;
- status and performance monitoring and logging;
- control actuation functions such as alarm reporting, remote control and data recording; and
- maintenance logging.

Hence, it can be seen that control and monitoring automation is at a similar or more advanced level than air traffic control automation. However, higher level problem solving and decision-making functions, such as system-level diagnosis, predicting faults from trends, reconfiguring systems in response to

system failures, or certifying systems and services, have not yet been implemented generally.

In many ATC centres an integrated centralised computer system (Control and Monitoring System [CMS]) is used to monitor and control engineering systems within ATC centres to help engineers to maintain the ATC service. The issue of supervisory control is already a day-to-day operational issue for system control personnel. Engineers monitor alarms from dedicated workstations and remedy faults either remotely (via software) or locally. Coupled with the increasing computerisation of ATM generally, ATM system control has adopted a 'soft-desk' environment, with VDU-based presentation of alarms and system 'mimics'.

Shorrock and Scaife (2001) note that the role of the ATM system controller actually has little in common with the tasks of the air traffic controller and is more akin to the control room operator of a modern nuclear power station. Since control and monitoring personnel are arguably as much involved in managing system disturbances as air traffic controllers, it is important to examine the impact of automation on system control. Whereas air traffic controllers tend to manage the *operational impact* of system disturbances, system controllers tend to rectify the *cause* and *spread* of the disturbance. However, Wickens *et al*. (1997) state that these roles and responsibilities may change with respect to supervisory control of automated systems and response to degradation or failure of the software and hardware that supports the automated functions. Perhaps, then, the air traffic controller role *will* need to expand to a more supervisory role, as is the case in other safety-critical industries. It may be that the air traffic controller and system controller of the future may be more closely aligned, or at least work and train in a more integrated fashion than today.

In contrast to the attention focussed on human factors issues in ATC, the human factors issues of control and monitoring ATM systems is a much neglected area (Shorrock and Scaife, 2001). Wickens *et al*. (1997) state that "the technicians who monitor and control the supporting equipment are typically provided with new monitoring and control devices that are tacked onto the array of such devices for other equipment in a loosely arranged combination that lacks integration" (p. 181). This has obvious implications for the management of system disturbances: while controllers may be provided with tools that have been designed according to human factors principles in a carefully change-controlled environment, their engineering counterparts may be working with tools designed without due consideration for the human user. This imposes a risk that system control and monitoring may, in fact, be the weakest link in the human factors chain.

Automation is as relevant to system control as it is to air traffic control. System controllers work with automation to monitor and control ATM/CNS systems, and are equal partners in the process of managing system disturbances. Therefore, the focus of human factors attention now has to spread to all of those involved in managing system disturbances.

1.6 Rationale

Since the human clearly has a number of vital roles regarding the 'management of system disturbances', effective human performance is just as important with 'automated' system as it is in more manually controlled systems. Hence, it is necessary to understand the implications of these roles on human performance.

This report provides a background to some of the known implications of automation on human performance in the context of managing system disturbances. These implications are complex and varied. In many ways it is impossible to separate the effects from the more general impacts of automation, such as on situation awareness, workload, trust, teamwork, skill changes and ageing. However, this report tries to deal with these issues only as they affect the management of system disturbances.

The aims of this work are as follows:

- provide a high-level framework which describes the process by which functional disturbances occur and people recover from these disturbances;
- review the human performance literature pertaining to the management of system disturbances, focusing on the roles of operational personnel and their recovery activities;
- conduct interviews in European ATC centres to contextualise the findings, and consider what kinds of failure occur, how they occur, how they manifest themselves and how they are recovered;
- develop a prototype recovery-oriented methodology by which to analyse human contributions to the management of system disturbances.

The background information describing the management of system disturbances was therefore derived from two sources:

- **Literature review** – A variety of papers were surveyed relating to recovery from failure.
- **Interviews** – 31 interviews were conducted with ATM personnel from four European centres. The interviewees spanned a variety of roles (see Table 2). The interview brief sent to interviewees prior to the interviews and the issues covered during the interviews can be found at Appendix.

The report is associated to an electronic tool available separately[2] to help analyse the process of managing system disturbances, called the **'Recovery from Automation Failure Tool (RAFT)**'. This is a group-based predictive approach to considering how people are likely to respond to system disturbances.

Section 2 of this report describes a model of recovery from automation failure itself derived from the literature and interview findings, along with the relevant findings from research and operational experience. Section 3 concludes the report. Details on authors and publications referred to in the report are provided at annex.

Table 2: Personnel interviewed regarding management of system disturbances

	Centre 1	**Centre 2**	**Centre 3**	**Centre 4**	**Total**
Facility Description					
Size of facility	Large	Large	Small	Small	
Location in Europe	Western	Northern	Eastern	Central	
Type of control	Area	Area, Approach	Area, Tower	Tower	
Personnel Interviewed					
Controllers (area or approach)	1	4**	2*		7
Controller (tower)			1*	1	2
ATC supervisors/watch supervisors	2	1	1		4
ATC watch managers	1				1
ATC safety managers		1	1		2
Incident investigation (ATC)		1			1
Operational engineers	3	2			5
Engineering watch manager	2		1		3
Other technical management	5				5
Incident investigation (engineering)	1				1
Total	**15**	**9**	**6**	**1**	**31**

* Another controller interviewed (now in another role) had experience in these roles too.

** One of these interviewees was a military controller. His interview was not considered further in order to better compare the information collected in the evaluation.

[2] Refer to the contact persons on page ii ('Document Characteristics') of this report.

This work provides background information, from literature and operational experience, on how people manage system disturbances. An accompanying Recovery from Automation Failure Tool (RAFT) can help to consider the process of recovery for new systems in a proactive way.

2. MANAGING SYSTEM DISTURBANCES – RESEARCH FINDINGS AND OPERATIONAL EXPERIENCE

2.1 The Recovery from Automation Failure Tool (RAFT) Framework

Research in the field of recovery from machine failures and human errors (e.g. Kanse and van der Schaaf, 2000) has highlighted a number of important factors determining the consequences of system disturbances. These factors include the following:

- **Context** – Any aspect of the operating context that can influence the failure or recovery process.
- **Causes** – The events or conditions that caused a technical failure.
- **Problem** – A technical failure or multiple failures, and an associated functional disturbance.
- **Effects and exposure** – The effects on the system or service, and the exposure in terms of time, aircraft, etc.
- **Recovery process** – The detection, diagnosis and correction of the failure, and mitigation of the disturbance, as well as any communication and teamwork required.
- **Outcome** – Monitoring of the effects of the recovery process, any further recovery actions required in case recovery was unsuccessful, any unwanted side-effects or complications and the ultimate outcome, which may be an ATC/engineering incident or an event with subsequent return to safe operation.

The relationship between these aspects is depicted in a contextual framework as Figure 1. The framework is useful in helping to understand and analyse system disturbances. It is based loosely on the framework proposed by Kanse and van der Schaaf (2000), but has been modified and adapted in several important respects to reflect the ATM context and the research literature. Hence, it is both a framework for the remaining subsections and the framework for the Recovery from Automation Failure Tool (RAFT). For the sake of consistency, the framework is referred to as **'RAFT Framework'**. The subsequent subsections therefore provide a detailed discussion of each component of the RAFT Framework, including literature, interview data and EUROCONTROL information.

When considering the management of system disturbances proactively, the whole picture has to be examined, including the system and work context, how problems arise and manifest themselves, the effects and exposure of problems, the recovery process, and the potential outcome.

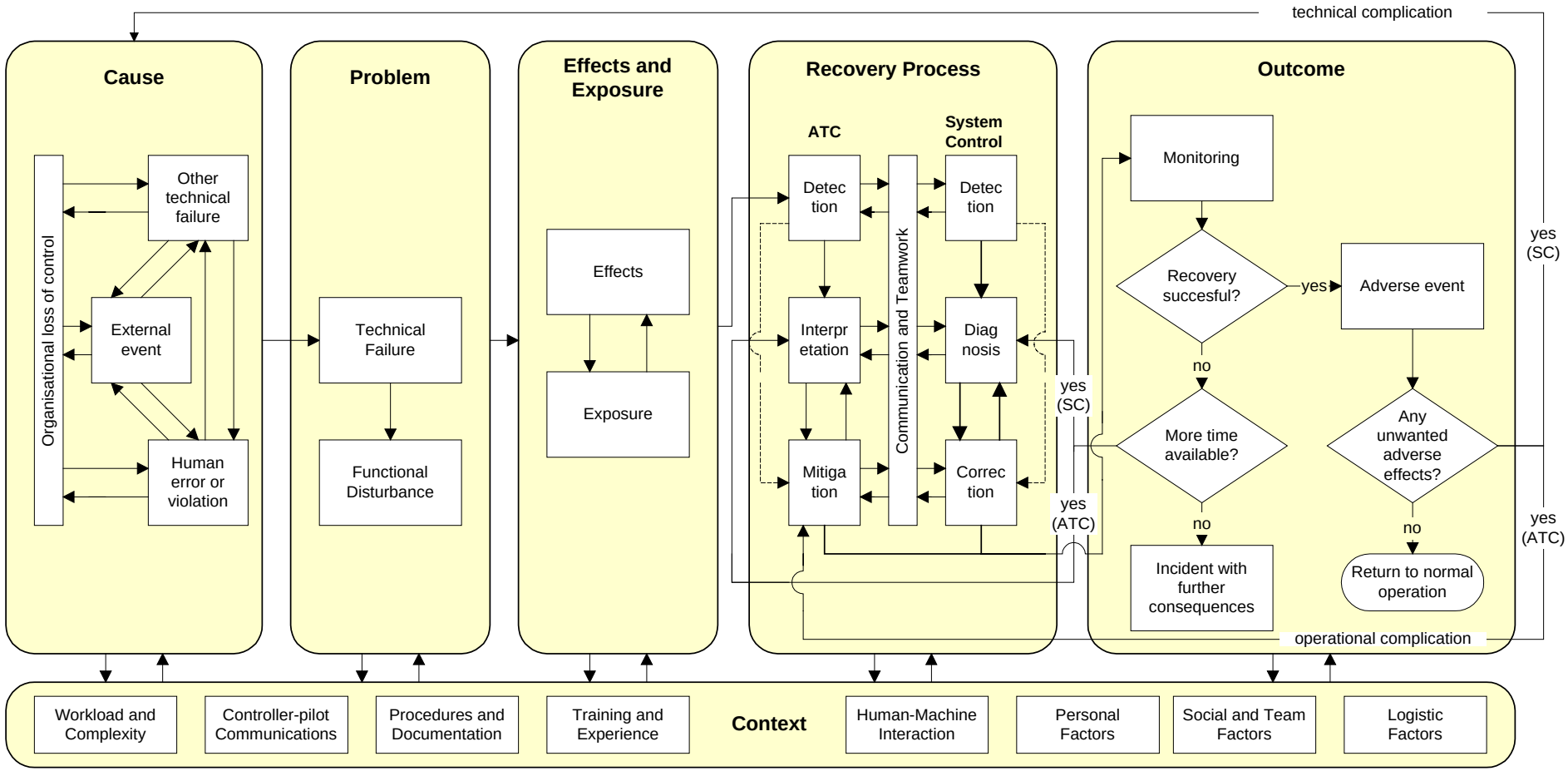
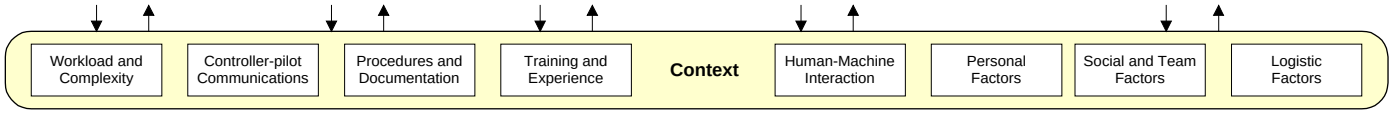


Figure 1: The Recovery from Automation Failure Tool (RAFT) Framework

2.2 Context



Context affects every part of the process of recovering from automation failures. In this sense, 'context is everything'. In the RAFT Framework, context has an impact on the following:

- **Cause** – Specific aspects of the total context will interact and filter through the organisation to create hazardous conditions or events.
- **Problem** – Contextual issues such as the human-machine interface will affect the manifestation of the failure as a disturbance.
- **Effects and exposure** – The effects and exposure of the failure and disturbance will be impacted by contextual issues such as the quality of pilot-controller communications.
- **Recovery process** – The recovery process is affected by many contextual issues, such as training and experience.
- **Outcome** – The outcome will be affected by workload and complexity factors (such as number of aircraft on frequency) and logistical factors (such as maintenance issues).

Few literature sources deal with contextual issues involved in managing system failures. However, it is reasonable to assume that many human factors issues affecting performance in normal conditions also affect performance in abnormal conditions and are probably even more critical. The following subsections introduce some of these issues, as represented in the RAFT Framework.

The following provides a very high level overview of the kind of factors that is likely to affect performance during system disturbances. This is not intended to be a comprehensive treatment, but rather an illustration of the kinds of issues involved. Since RAFT is a recovery-oriented approach, in this project, the focus is primarily on the contextual factors affecting *recovery*, rather than contextual factors that can cause failures.

2.2.1 Task load and system complexity

A key reason for automation is to increase capacity and optimise the workload of the human operator, whilst maintaining the safety integrity of the total

system. Different functions in ATM can be automated, and so mental workload effects may be seen in relation to these different functions. Automated information integration and inference provides better information to controllers and thereby reduces excessive workload, primarily via reduced working memory demands. Automated ATM systems with functions that draw inferences about future events (prediction) can provide assistance to improve decision-making and may decrease workload associated with thinking and interpretation (Harwood *et al*., 1998; Wickens, 1999).

Some researchers have suggested that overall workload may not be reduced by automated assistance provided, even under full automation (Billings, 1991; Wiener, 1985). It has been proposed that there is actually a shift in the *type* of workload such as a greater monitoring load. When automation is implemented, operators may incur additional workload associated with input devices, errors, intrinsic 'automation-management' tasks and unexpected and new peripheral tasks needed to use the automation. New ATM tasks may also require more time to think about and understand the options or decisions generated by the automation. Moreover, such knowledge-based thinking may interfere or compete for mental resources required for other ATM tasks.

Different levels of automation may also affect workload. Intermediate levels of automation keep the human involved in system operation, and may result in better work system performance and lower workload compared to highly automated systems (Endsley and Kiris, 1995), which makes higher monitoring demands of the operator.

The research findings on the impact of automation on workload appear inconsistent and inconclusive. If workload is too low, air traffic controllers and system controllers may be too out of the loop to properly intervene, while if workload is too high, then personnel will not have the physical or cognitive capacity to perform recovery tasks, in light of the demands of the task. For system control personnel, workload will tend to peak when multiple failures occur (Wickens *et al*., 1997). Under such situations, system control personnel will have to detect the failures, some of which may be masked by higher-order failures, diagnose the cause of the pattern of failures, assess potential solutions and execute appropriate actions, potentially under intense time pressure.

Some controllers interviewed stressed that many of the failures they had experienced were much worse under conditions of high traffic load or complexity, or both.

The level and type of automation can affect the level and type of workload experienced by the human. Overall workload does not necessarily reduce with automation; a shift in the type of workload may occur instead. Automation can also increase the level of system complexity. These factors need to be managed.

2.2.2 Pilot-controller communications

Pilot-controller communications will continue to be a critical factor affecting the handling of system disturbances in the future. The effectiveness of communications is now a key issue for the handling of aircraft emergencies. Any potential problems with automation reliability will increase further the criticality of communication. Any failure tends to affect communication workload, and it is crucial that the method, content and quality of communication is appropriate. Even with the introduction of data-link, rapid and instantly-available means of communication such as Radiotelephony (R/T) will clearly be necessary to provide emergency communication, both informing pilots of the disturbance and providing action to maintain safety.

2.2.3 Procedures and documentation

Procedures are another critical enabler for effective recovery. Procedures are required not only for 'normal' operations, but also for 'abnormal' operations such as those involved in managing system disturbances. Procedures must be designed to facilitate a smooth transition from normal operations to fallback operations and back to normal operations. If no procedures are available to cover all foreseeable system disturbances, then the controller or team has no choice but to use his, her or their own mental model(s) of the system and operational environment to perform recovery actions. Such *ad hoc*, knowledge-based behaviours may be contrary to those that might be planned in advance. Assuming that comprehensive procedures are available, they must also be accurate and up-to-date, realistic, clear and easy to use, accessible, and linked to training.

Experiences in other industries with highly automated systems reveal also that procedures have to be adjusted to the diagnostic tasks the user has to perform in a disturbance. Nuclear has invented the distinction between 'symptom-based' and 'event-based' procedures (e.g. Straeter, 2000). While event-based procedures are related to a certain type of disturbance (e.g. loss of secondary radar), symptom-based procedures guide the user to the correct actions in case of unclear causes for a situation (e.g. behaviour of a/c on radar screen not according to control instructions). The reason for introducing symptom-based procedures is that users are not capable to deal with too many event-based procedures in a given situation and applications of wrong event-based procedures may lead to serious consequences in term of safety.

While procedures existed for aircraft emergencies in all of the centres visited, procedures to help controllers deal with ATC system failures existed in only two of the centres visited. Checklist-type procedures have been developed from these formal procedures and these were examined in one centre. In this centre so-called 'fallback briefs' exist for all identified fault scenarios based on operational safety hazards, hence forming a link to risk assessment. These are issued to ATC personnel (controllers on all sectors, watch supervisor and watch manager) to help them recover to a steady state. Thus, if, for example, radar services fail on all workstations, personnel have a readily available guide

to help them recover from the failure. These fallback briefs vary according to the type of user, because different roles may require different information on system failures and recovery procedures. The procedures capture the key effects of the failure on the operational system and the steps the person must carry out to recover and ensure the service continues to be safe. Some of the procedures have been used successfully and are constantly under review. In the other centre that had recovery procedures available, checklists exist on all workstations on how to use the backup system. In one centre without such procedures, some controllers stated that checklists would be useful. In this centre, similar checklists already exist for aircraft emergencies and building-related problems (e.g. fire, bomb threats).

While procedures were available in two of the centres visited, controllers may not be familiar with them and may not have received refresher training. If a procedure needs to be checked during operations, support staff would do this. Some personnel stated that infrequent problems are dealt with on an *ad hoc* basis until a procedure is devised.

Good procedures are critical when managing system disturbances. The alternative is that human performance will be more variable and may not necessarily be appropriate. Good procedures are comprehensive, accurate and up-to-date, realistic, clear and easy to use, accessible, and linked to training.

2.2.4 Training and experience

Automation can reduce manual skills by removing the person from active, in-the-loop control, and removing the opportunities for practice that are so vital in the maintenance of skills (Bainbridge, 1983; Parasuraman *et al.,* 1993; Wickens, 1999). However, the need for manual skill remains as long as the potential remains for humans to intervene in the case of a disturbance. This means that controllers may not have the skills and experience required to intervene manually in the case of automation failure. Controllers must therefore have regular training in recovery-related tasks, to ensure that competence and confidence are maintained at appropriate levels.

According to Wickens *et al*. (1997) automation is changing the job profile of the systems controller, from a person with knowledge of hardware for specific equipment or systems, to knowledge of and responsibility for monitoring and controlling interactive systems, management of software-intensive, distributed-networked resources, and application of systems engineering methods to provide system services to users. Automation-related skills and knowledge are integral to this. Training for recovery will in future need to be more integrated, interactive and system-wide, in contrast to the previous focus on independent equipment and subsystems.

In one of the centres reviewed, a variety of measures are in place for training that relate to management of system disturbances, including:

- a licence and ratings system for subsystems, for engineering staff;
- critical incident stress management programme;
- refresher training in handling emergency flights for controllers (but not in recovery from system failure);
- monthly engineering training for software errors and maintenance;
- joint training for engineers and controllers;
- twice per month use by the controller of the telephone backup system for practice.

However, controllers at this centre were not actually trained in dealing with disturbances. It was stated that there may be problems if controllers have not experienced a particular failure before. Most would use their best judgement, but this will depend on experience, and experience will vary. Controllers need to keep in mind the priorities (separation, continue flight, etc.) and quickly find a workable solution rather than evaluating every alternative. Interestingly, in two of the four centres, it was stated that older controllers were trained in 'conventional' or procedural control, but newer controllers are not. In one of these, one interviewee noted that he had previously experienced many communication and radar failures with older systems. In these times, paper job aids (tables and charts) were on hand as a 'backup' measure. Another controller stated that the procedural control course at EUROCONTROL's Institute of Air Navigation Services (IANS) was very helpful and recommended that it should be maintained as course for system disturbance management.

Personnel in two other centres stated that new controllers practise working in conditions of radar failure and SSR failure during initial training and thereafter during annual continuation training, which also covered aspects of technical system performance. However, it was stated that controllers should be exposed to all known types of failure in training.

In another centre it was found that there is little opportunity for personnel to practise coping with known occurrences in a simulated environment, even where procedures exist for such occurrences. There was some concern that, since the need to recover from serious system failures was very rare, personnel had little experience of having to perform recovery activities. Paradoxically, although new systems appear more reliable, it was considered that this deprived controllers of the opportunity to learn to recover from disturbances, and this opportunity needed to be designed into their experience via training. The importance of rehearsal and training was brought up by a number of those interviewed. However, it is understood that a package of advanced fallback training is presently being developed at this centre.

Some of the controllers identified what they perceived as future problems. First, it was believed that future controllers would have more difficulty in forming the 'picture' of the traffic situation. Second, it was thought that the future controller might – more than today – require a mental model of the ATC technical system. Third, younger and older controllers had different perceptions of one another: younger controllers were perceived by some older controllers to be more trusting of the reliability of new equipment, having rarely experienced failures in the past, while older controllers were perceived by some younger controllers as less computer literate and more suspicious of technology.

The more passive nature of work with automated systems can result in a loss of manual skills and reduced opportunity to practise skills that might be required to manage system disturbances. This lack of experience increases the requirement for various forms of continuation training and disturbance simulation to maintain competency and confidence, and to help calibrate trust in the system.

2.2.5 Human-machine interaction

Human-machine interaction is an obvious contextual factor affecting recovery from automation failure. Norman (1990) has emphasised the role of appropriate feedback and interaction in the success of automation. The human-machine interface must both keep the human in the loop by presenting required system information in a clear and comprehensible way during normal operations and make clear abnormal or disturbance information, to allow personnel to detect, diagnose, correct and mitigate the failure. One significant change will be the increase of alarm handling in ATC. This activity will need to be integrated with the controller's work, which may present problems in light of the very short timeframes involved in ATC compared to other industries where alarm handling is a key performance issue (e.g. nuclear, chemical).

A problem for one centre would be detecting faults causing degradation of system performance that are not highlighted to system control engineers via the Control Monitoring System (CMS). The system has been designed to detect most faults, but subtle problems may not be detected in a timely fashion. In fact, it was reported during interviews that system control personnel receive a multitude of warnings, most of which need no action, as the system self-corrects. In another centre one controller stated that new functionality was sometimes not necessary and not used, and can make the system unnecessarily complex (e.g. finding a required function).

The human-machine interface must keep the human involved in the task in a meaningful way, making both normal and abnormal clear and understandable, while providing the time and appropriate means to act.

2.2.6 Personal factors

The state of the individual is another important determinant of response under abnormal conditions. For instance, fatigue can impair a person's ability to detect problems, excessive trust may lead to personnel doubting their own judgement and abilities, or panic may affect decision-making under time pressure. Such factors need to be examined in advance to ascertain the likely condition of the person *in situ*, rather than assuming that all personnel are optimally rested, confident and calm, for example.

One personal factor mentioned in one of the centres related to a risk that emerging trends may not be picked up due to complacency or over-confidence in the control monitoring system, particularly if the CMS fails to highlight a failure (see Section 2.2.5, 'Human-machine interaction', above). Another controller in another centre stated that critical incident stress management is essential in managing the stress associated with disturbances.

Different people may deal with abnormal situations in different ways, or the same person may react differently over time or in different contexts. Many personal factors can be foreseen, and their manifestation, likelihood and impact can be managed.

2.2.7 Social and team factors

Team coordination and communication is without doubt a critical factor in increasing recovery success. Managing system disturbances is, perhaps more than many other ATM tasks, a team effort. Automation often leads to changes in levels and kind of 'tacit knowledge' in the activities of colleagues, for instance by increasing the 'black-holing' effect, where a controller becomes fixated on the human-machine interface to the cost of the human-human interface. Controllers will need to cultivate 'shared situational awareness' if recovery is to be successful.

Critically, both ATC and system control need to coordinate to ensure that aircraft are handled safely and that systems are brought back on line as soon as possible. For instance, a controller may notice a disturbance and inform the supervisor. The supervisor may inform system control, ascertain which other controllers are affected by the problem and communicate the disturbance to these controllers. System control will need to inform the supervisor of the nature of the problem and provide an estimate of time to repair. System control may then inform the supervisor that the function is again working properly and this information will be relayed to the controllers. Team members must therefore trust each other, have adequate supervision and support, and have appropriate means of communication.

On the issue of social and team factors, interviewees in one centre stated that staffing during of a major disturbance would be a problem, because there are

currently just enough personnel to cover all working positions. Hence, it is difficult to release staff for simulator training, and so staff may never have experienced particular failures in training.

Interviewees from another centre stated that good communication and teamwork is essential between the ATC and system control. At the start of each shift, any system outages are brought to the ATC watch supervisor's attention by his counterpart in system control. Any reduction in the level of redundancy is also highlighted. Facilitating rapid and clear communication between ATC personnel, systems engineers and those at other units and sites when problems occur can be difficult. Procedures are in place, but depend on all parties working together optimally. An Air Traffic Incident Coordination and Communication Cell (ATICCC) is established in one centre visited, which is manned by key personnel when serious problems (including system failures) occur. One controller reported that cooperation with technicians could be improved at his centre, as the official reporting line was perceived as inefficient (from controller to supervisor, supervisor to system manager and system manager to technician). This controller also stated that feedback from technicians could be improved.

During a disturbance teamwork increases both within teams and between teams, particularly between ATC and system control. Effective communication and coordination increase team situation awareness, linking together the processes of prevention, detection, interpretation/diagnosis and mitigation/correction of problems.

2.2.8 Logistical factors

Logistical factors that are likely to affect recovery success are likely to include maintenance and staffing issues. Maintenance issues will include maintenance philosophy, maintenance scheduling, assignment of the technicians, proximity of equipment, availability of tools and parts, job training aids, and availability and operability of test support equipment. Staffing issues will include the requirement for, availability of, and assignment of personnel both for normal and abnormal operations. One crucial question is, if staffing requirements are determined partly according to automation, then how are the increased staffing needs during system failure fulfilled?

2.2.9 Other organisational factors

Other organisational factors include organisational communication. Interviewees in one centre stated that safety-related information is communicated via safety briefings, bulletins, news, safety panel, and technical and flight data personnel. Two years ago two workshops were held in the same centre as part of a redundancy study to investigate potential failures. In another centre, during design and development, a full hazard identification process was undertaken, considering both the failure modes and potential

consequences. The hazard identification process identified the systems and services, associated hazards and assigned a hazard severity category and risk classification with associated probability target to each hazard. For the operational ATC system, a set of Operational System Hazards (OSH) were derived with implicit safety requirements.

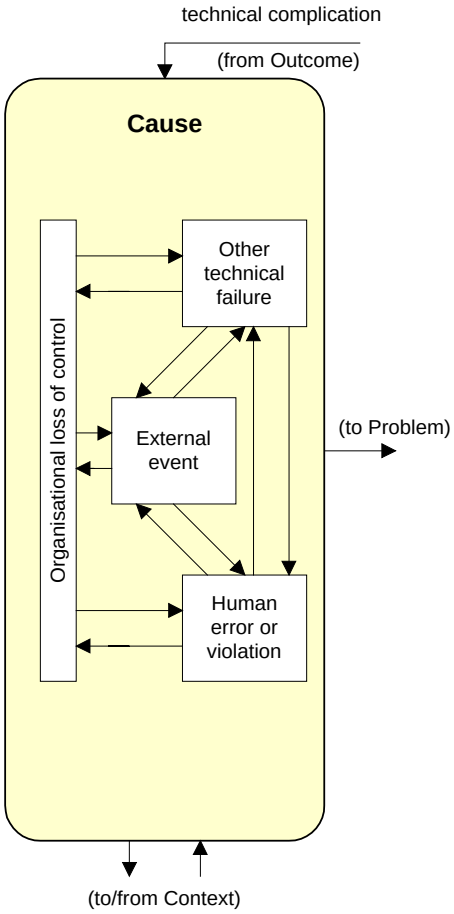
At this centre risk management and hazard identification has pinpointed the vast majority of such single point failures and appropriate safeguards have been implemented. Highlighting further single point of failure components in the system is an ongoing process. For instance, it was recently recognised that system error messages could congest one of the Local Area Networks (LANs) used by the system, even if a component has not totally failed (i.e. it may be reporting problems). This congestion could potentially lead to a loss of all workstations on the LAN, i.e. forty adjacent workstations. System control would only receive one warning (which could be 'lost' amongst other warnings). This hazard has now been addressed.

Safety performance monitoring is an essential element in the delivery of safe ATM. The system control room is manned constantly and allows engineering personnel to monitor systems problems – both those that are automatically rectified and those that need human intervention (such as the replacement of hardware or modification of software). The performance of the operational systems is subject to regular hazard review meetings, where recent system problems are assessed for their impact on safety.

Controllers in another centre had difficulties in communicating system problems and safety issues to their management and to technicians. They explained their problem to the local authorities. These analysed the radar system, then approached the management with a change request.

Organisational communication is critical to achieving and maintaining good performance in managing system disturbances. Problems can be foreseen and prevented, and solutions can be shared and communicated, so that unwanted surprises are less likely.

2.3 Cause



The causes of failures according to the RAFT Framework stem from several interacting sources, as described below.

2.3.1 Organisational loss of control

Ultimately, most or all failures can be traced back to a loss of organisational control, for instance at the levels of design, construction, commissioning, maintenance and management. Organisational loss of control therefore involves a failure to set or maintain compliance with adequate standards (for maintenance, inspection, work permits, engineering, change management, materials, risk assessments, housekeeping, environmental control, etc.) For instance, a requirement specification may have omitted crucial requirements, or a programmer may fail to code according to the specification. Maintenance standards may not be maintained, or an engineer may perform work incorrectly and without subsequent independent checking. Management may purchase systems or software that conflict with existing systems or software. Even where a failure is caused by an external event, such as weather, it is the duty of the organisation to protect against such events as far as reasonably practicable.

2.3.2 Other technical failure(s) or fault(s)

A failure that leads to a disturbance may be caused by an upstream failure. Leveson (1995) gives the example that a relay may close at the wrong time due to the improper functioning of some upstream component. In this case the relay has not failed but untimely relay operation may well cause the entire circuit to enter an unsatisfactory state. This event is called a fault.

Interviewees in one centre stated that there were various code-callsign databases and a fallback system. Sometimes controllers may get additional data, e.g. duplicate flight plans, codes or callsigns. Squawks sometimes switch so that an aircraft appears in an erroneous position. Sometimes squawks may not be correlated. At one centre this information can be lost due to system overload and too much VFR traffic; there are only a certain number of tracks which the system can process.

Controllers interviewed at another centre experienced a computer failure within the Radar Data Processing (RDP) system, which resulted in a total loss of radar services for a period of hundred seconds early in the morning.

Loss of power supply is very unlikely in the three ATC centres visited due to modern uninterrupted power supply systems (e.g. diesel generators and battery backup). However, this has happened several times (see examples below) and has caused particular problems when this is a single point of failure.

➘ Example – Loss of power supply 1
On the evening of 6 July 2000 at a period of peak activity the main power and the backup power for the Sydney air traffic control system failed. The power outage lasted for about two minutes and it took another ten minutes to reboot the computers. The fallback strategy involved pilot-to-pilot communications and predetermined holding patterns.

➘ Example – Loss of power supply 2
On 15 January 1999 at 14:00 the power failed at Seattle en-route ATC centre. The power failed during a normal, routine quarterly test procedure on the power supply units when there was a very brief (less than one second) interruption of the power supply. The computers had to be rebooted and recalibrated, and the communication systems failed, since these were computer-dependent, digitised and touch-screen interface modules. This system took over a half-hour to reload. The main radar displays and the backup display system entered a fault state. It took between 45 and 75 minutes for the radar displays to come back at various sectors. Controllers used a hard-wired, emergency radio backup system with paper strips and were able to restore limited ATC service within a few minutes.

2.3.3 Human error and violation

Wickens *et al*. (1997) argue that the contributions of both automated equipment and its human users to the cause, complication or resolution of major outages should be considered. Human error by system controllers, engineers and maintenance personnel might result in a technical failure. An engineer, for example, may switch off the wrong system, remove the wrong component, or make an error that makes matters worse when trying to correct a problem (so called ‘errors of commission’). Personnel might also ‘bend the rules’ (so called ‘procedural violations’) in maintaining systems, perhaps because a procedure is not seen as useful or necessary, and therefore work outside of the boundaries of operation that are known and understood by the organisation. It is possible that the rule is a bad one and so should be formally abandoned. In other circumstances rule breaking is akin to running in the dark. Errors made in this ‘uncharted territory’ may be particularly dangerous.

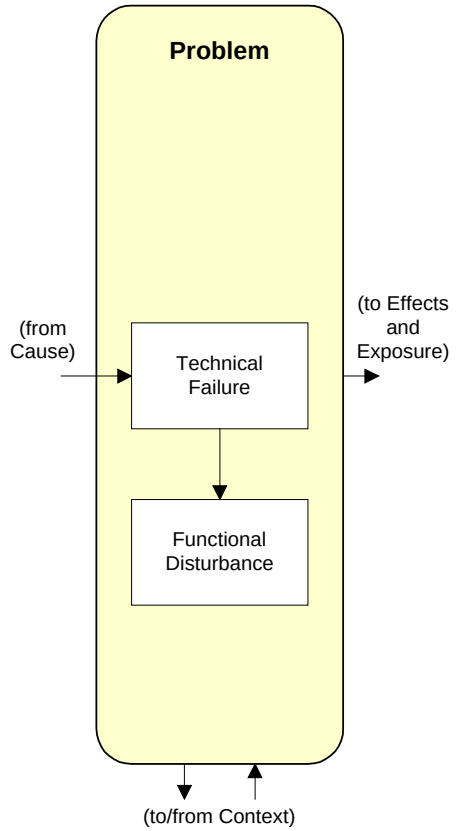
2.3.4 External events

There may be instances when unfortunate, unforeseen and uncontrolled events cause a failure. Examples include the effects of severe weather (e.g. flooding), fire, industrial action, accidents, vandalism and terrorism.

As an example of an external event cause, an incident occurred at one of the centres visited where an electrical cable connected to the Flight Plan Processing (FPP) system was cut accidentally. In another case a fire in the telecommunication equipment room caused the loss of sixty communication lines.

Human errors or violations, external events, or other technical failures can act independently or in collaboration to cause a technical failure. Ultimately, all of these causes can be traced to an organisational loss of control.

2.4 Problem



2.4.1 Technical failure

A technical failure is the result of interacting causes. It is defined as follows:

*A **failure** is the non-performance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions (Leveson, 1995).*

Leveson distinguishes two causes of failure in physical devices:

- Failures may be caused by design flaws, where the intended, designed and constructed behaviour does not satisfy the system goal.

- Alternatively, failures may result from a deviation from the originally designed behaviour, for instance due to wear-out, fatigue or degradation over time.

Leveson also distinguishes three types of failure:

- *Early failures* occur during the debugging or burn-in period. They are due to poor assemblies or weak and substandard components, or to software problems. Such failures may be associated with faulty assumptions about the operational environment and will gradually be eliminated until the failure rate reaches a constant level.

- *Random failures* result from complex uncontrollable and sometimes unknown causes. The failure rate is assumed to be constant during this period, known as the 'useful life' of the system.

- *Wearout failures* begin when components are past their useful life and the malfunction rate increases sharply. These failures are hardware-related, though software modification and maintenance may cause a seemingly parallel effect. However, in reality problems occur when software is modified is more closely related to early failures, since the new version is essentially a new design.

There are various types of technical failure in ATM, which can be classified in various ways. The following provides one example:

- total loss of data, e.g. workstation failure,
- partial availability of data, e.g. no SSR, R/T interference,
- loss of redundancy, e.g. single radar source, fallback mode,

- loss of data integrity, e.g. code-callsign conversion problems,
- data corruption, e.g. text corruption, graphics card problems,
- extra data, e.g. ghost tracks/radar reflections,
- performance timing problem, e.g. late coordination requests.

It is also necessary to define the *engineering* definition of error:

*An **error** is a design flaw or deviation from a desired or intended state* (Leveson, 1995).

In engineering terms a failure is an event (a behaviour), while an error is a static condition (a state), though this does not apply to human errors. Programs, designs and models that do not operate (but have states) can be erroneous, but do not fail. An error may lead to a failure in an operational device and a failure may lead to an erroneous system state.

It is important that the understanding of term 'failure' is not restricted to catastrophic system failures. Small, infrequent problems can combine or act in isolation or cause a disturbance or an unstable system. According to Wickens *et al*. (1997) such problems can be produced by software bugs, errors in data transmission or storage, timing errors, and subtle design deficiencies not detected in formal acquisition tests.

It is interesting to note that it is rare for automation to fail outright or catastrophically; failures are often exhibited at a new level of complexity. For instance, a flight strip printer might fail, therefore (and obviously) no longer printing strips, while an electronic flight strip may display credible but erroneous data. The second failure may be the most serious. Alternatively, automation may perform as designed, and yet still bring the system into a hazardous or faulty state. In a survey by the US Aviation Safety Reporting System (ASRS), about incident reports involving automation, Mosier *et al*. (1994) reported that automation was doing exactly what it was supposed to in a majority of these incidents.

Technical failures can be classified in various ways, but most failures do not involve outright unavailability. More often failures will take a subtler form, which could be equally or more serious or troublesome.

A ***fault*** is a higher-order event. If a component does not operate due to an upstream failure, the component in question has not failed, but may cause the system to enter an undesirable state - this event is called a fault (Leveson, 1995). All failures are faults but not all faults are failures.

Many would argue that software does not 'fail', since software is the design for a (special purpose) machine, not a machine in itself. However, this is only true for a narrow definition of 'failure' (Leveson, 1995), in terms of a physical device. Software does not degrade due to wear or fatigue; it operates in the way that it is programmed, normally in the way that the software engineer

intended. Hence, ***software-related computer failures*** are always *systemic* – they are caused by design flaws, not deviations from originally designed behaviour. But computers can behave in hazardous ways, not intended by the designer, or expected by the user. Indeed, compared to hardware, software behaviour is much more unpredictable, with a large number of incorrect behaviours.

2.4.2 Functional disturbance

According to the RAFT Framework, a technical failure leads to a functional disturbance at the operational level.

*A **functional disturbance** is the non-performance or incorrect performance of an automated operational function.*

At this level the failure affects the controller because one or more automated functions are impacted by one or more technical failures. Such functions may for example include cueing, prioritisation, option generation, output or reminders. These functions may be affected in various ways, illustrated by the following 'functional disturbance modes':

- timing, speed, duration (early/late, fast/slow, long/short), e.g. 'prediction too late';
- availability/occurrence (not, part, repeat), e.g. 'reminder not provided';
- quality (incorrect, vague, misleading), e.g. 'prioritisation incorrect';
- object (right function wrong object), e.g. 'reminder sent to wrong controller';
- sequence (out of sequence), e.g. 'choose option out of sequence' (before controller confirmation).

2.4.3 Interview findings

Controllers in the four centres experienced functional disturbances infrequently. In one of the centres controllers have been working with the (radar and Flight Data Processing [FDP]) system for two years without an incident due to system failure. In another centre the interviewees stated that, although the system was quite new, it was very reliable compared to the old system and very few failures had been experienced. There is a high level of designed-in redundancy in all centres' operational systems, such that the failure of any system is automatically and seamlessly overcome by a duplicate standby system. A good example of this is the power supply system which in one centre consists of two separate external mains electricity feeds, backed up by generators and batteries capable of sustaining all equipment for several hours. Furthermore, equipment is wired so that duplicate systems are powered from different supplies. In this centre, there are two identical equipment rooms, such that degradation or failure of any system in one room

(say of a RDP computer) will lead to its counterpart automatically taking over with no interruption. Therefore, these safeguards mean that it is unlikely that any system failure will result in a serious loss of the air traffic controllers' facilities. The system is designed so that as far as possible, there are no areas where 'single point failures' could result in system failures. This means that there should never be just one failure leading to a major operational disturbance. The system has been designed so that many combinations of failure have been predicted and accounted for.

ATC centres generally operate a redundancy philosophy, duplicating systems so that technical failures do not lead to a function disturbance.

Another factor that reduces the likelihood of failures in this centre is a parallel system that constantly shadows the main system, allowing anomalies and inconsistencies in data to be highlighted and automatically reconciled. Also, most systems have been specified to run routinely at only a fraction of their maximum capacity. Thus, radar display processors only use 50% of their maximum output[3].

The result of the redundancy, backups and integrity checking is that in the majority of cases, a system failure should not result in a problem that impacts upon an individual controller's ability to carry out their tasks safely. In the majority of cases, when a system problem is encountered, the fault is automatically rectified with no interruption of service to the controller. In fact, it is what might be considered relatively 'low severity' failures that may inconvenience the controller. For instance, failure of a keyboard or mouse at an individual workstation cannot be rectified automatically by the system and will normally require a controller to move to another workstation until the hardware is repaired or replaced.

Various system disturbances were discussed by the interviewees in the three centres. Some of these were problems that had actually occurred, others were problems that could occur (e.g. that were identified in a risk assessment). Some current problems that can impact directly on air traffic controllers are described below.

Total loss of data/function

- *Total loss of Radiotelephony (R/T)* – Radio is the key tool by which controllers communicate with aircraft under their control. It may be extremely unlikely that all R/T frequencies will fail simultaneously on all sectors. However, the effect on controllers and pilots would be the loss of air-ground/ground-air communications.

[3] In another centre visited, however, equipment was housed in the same room and duplicate systems (e.g. servers) were housed in the same cabinets.

➘ Example – VHF failure
On 3 April 1997 the Transport Accident Investigation Commission (TAIC) of New Zealand issued a final report about a failure of the ATC communication system in the Christchurch Area Control Center. During the event the Airways Corporation communication network system suffered a failure that caused a temporary loss of all ATC Very High Frequency (VHF) radio communications in the Wellington Sector. The investigation found that the Airways Corporation communication network failure was the result of software maintenance action, and the consequent failure of the VHF channels was associated with the architecture of the system, which compromised the available diversity. As a result of the findings TAIC issued a recommendation to the Director of Civil Aviation asking for a review of the 'Emergency' section of the Instrument Flight Guide to ensure that the section on 'communication failure' provided pilots with sufficient information and advice on actions to take in the event of a failure of communications from ATC.

- *Total loss of radar* – Controllers interviewed at one centre had not experienced this. Newer controllers at this centre are told that total loss of radar is not possible and are therefore not trained to deal with such an event. Controllers at the second centre stated that, although unlikely, a total loss of all radar services could occur for a number of reasons, but it should never occur due to a single point of failure. If all information from all radars is lost, all radar pictures at this centre will be frozen and a yellow cross will be overlaid onto the display. Functionality of electronic strips is degraded. Controllers at the third centre experienced this frequently more than two years ago, before the implementation of a modern and more reliable system.

- *Workstation failure* – Single workstations sometimes fail. In all three centres most workstations have a main and a fallback mode. The fallback mode has fewer or different functions and a different display (e.g. different callsigns, more colours, no Short-term Conflict Alert [STCA]). The redundancy arrangements at some centres mean that it is possible to loose every second radar display. This can occur due to complete loss of one hub or one giga-switch. Controllers either use fallback mode or share the coordinator's display.

- *Flight Plan Processing (FPP) problems* – Controllers at all three centres identified FPP problems (no plan or late plan). When controllers at one centre lose FPP functionality, the system blocks data, and automatic coordination is not possible (data may not be passed following an estimate). In another centre a national FDP system transmits data to a local server, which collates, stores and distributes the flight data received to the workstations. The FDP system could fail (a single failure point), or the link between the FDP system and local server could fail. The unavailability of FDP system or the breakdown of its link to the local server would mean that the FDP data would be unavailable to all workstations,

and so no new flight plans would not be received. Controllers learn of this problem when a brown border appears on the display. This affects route processing, callsign pairing with track data blocks and functioning of a controller assistance tool. In addition, electronic coordination and automatic production of paper flight progress strips would not be possible.

➘ Example – Failure of FDP system
There were four failures of the National Airspace System (NAS) in 2000 at West Drayton. On 17 June 2000 the UK NATS' FDP failed for several hours. Two days prior to the failure, new configuration parameters had been installed on the system to improve flight strip printing for controllers at Prestwick and this triggered a latent software error. The main reason for the extended delay in restoring full service was the failure of linked communication systems and the need to rebuild the data in these systems. The causes of the failures were established within a short time of each event and a combination of software fixes and other preventative actions were identified, tested and implemented. Following the events of 17 June new system design constraints were introduced to prevent the failure of linked systems (Source: NATS, 2000).

- *Loss of local flight data server* – The local flight data server at one of the centres collates and stores flight data received from the FDP system and distributes this information to the workstations. If the local flight data server fails, the central flight data source is lost, including the link to the FDP system and ability to pass electronic information to other units. The effects would be similar to those described in the previous bullet (e.g. regarding electronic coordination and new flight plans). Furthermore, in this situation, it would not be possible to combine or spilt sectors, or to sign on or off a workstation.

- *Failure of speed and sequence information tool* – One of the centres visited uses a tool which gives speed and sequence information for area and approach control. If this fails, controllers must return to manual and telephone operation.

- *Communication line failure* – One centre reported the loss of sixty communication lines (data and communication), but each line has a minimum of one redundant line.

Partial loss of data/function

- *Loss of Secondary Surveillance Radar* (*SSR)* – Loss of SSR would mean that only primary data was shown on the display.

- *Loss of Multi-radar Processing (MRP)* – At each of the three centres each controller's radar picture is the product of a number of selected radar sources (e.g. 2, 3 or 4) at one centre; the MRP system collates the radar data and also provides the data necessary for the functioning of the short

STCA. If MRP should fail, all radar pictures would be frozen (i.e. not updated) and all Tactical and Planner controllers would see a yellow cross appear over their radar display.

- *Loss of Single Radar source/Processing (SRP)* – In one centre visited it was reported that, typically, only the sector assistant would rely on a single radar source. However, in certain fallback situations, sector controllers would have to rely on a single radar source. Controllers stated that if a workstation used a single radar source that fails, the radar picture would be frozen and a yellow cross would appear over the radar display. If a workstation used the failed single radar source as part of its MRP, there might be a reduction in coverage (if an aircraft is in a region of the sector airspace covered by just the failed radar source).

Loss of redundancy

- *Loss of backup R/T frequencies* – One centre reported the loss of many backup R/T frequencies due to a fire.

Loss of data integrity

- *Code-callsign and squawk problems* – Controllers at all three centres reported that code-callsign and squawk problems sometimes occur. Controllers can be presented with additional spurious data, e.g. duplicate flight plans, double code or callsign. Squawks can be switched so that two aircraft appear to switch positions. In one centre this can occur when aircraft pass close to one another. In another the problem was caused by an error in the code-callsign database.

Data corruption

- *Data corruption* – Interviewees at one centre reported a problem with graphics cards (bad oscillation), causing corruption of text and graphics.

Extra data

- *Ghost tracks* – Two centres reported that ‘ghost tracks’ (duplicate tracks) had occurred on radar displays.

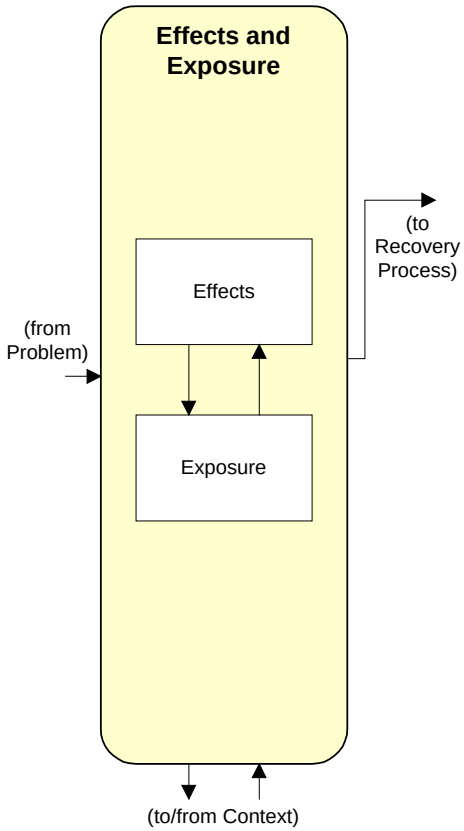
- *Loss of Basic Global Services (BGS)* – BGS is an element of one centre’s Control and Monitoring System (CMS). This has an immediate effect on ATC when there is a requirement to move, combine or split workstations.

Performance timing problems

- *Flight progress strip printing problems* – Controllers at one centre reported receiving strips late (after the aircraft has entered the sector) due to software problems.

In future the potential problems of ‘loss of data integrity’, ‘data corruption’, ‘extra data’ and ‘performance timing problems’ will probably increase proportionately, while problems associated with ‘total loss of availability’ and ‘partial loss of availability’ of data or functions will probably decrease proportionately. This prediction is based on the observation that software will be used more, and this is subject to errors and unexpected interactions. However, hardware is becoming more reliable and system philosophies involving increased redundancy are now the norm.

2.5 Effects and Exposure



The disturbance of a system function could impair the safety of the air navigation service and subsequently could impact aircraft operations.

The EUROCONTROL air navigation service Safety Assessment Methodology (SAM) proposes a 'cause-consequence' approach to determine the effects of the loss or degradation of system function(s). To support the classification of a hazard's effect severity, three sets of severity indicators are proposed:

- Set 1: Effects on air navigation services,
- Set 2: Exposure,
- Set 3: Recovery.

The following text deals with sets 1 and 2, and is adapted from the relevant report (EATM, 2004e).

2.5.1 Effects on air navigation services

The effects on air navigation services are broken down into four components:

- **Safety of provided air navigation services:** Effects on the ability to provide or maintain safe air navigation service(s).
- **Working conditions:** Effects on the controllers and flight crew ability to cope with the reduction in functional capability, especially, impacts on their workload.
- **Adverse operational and environmental conditions:** Effects on the ability for controller and/or flight crew to cope with (other) adverse operational and environmental conditions.
- **Functional capabilities:** Effects on the functional capabilities of the ground part of the ATM system and aircraft functional capabilities.

2.5.2 Exposure

- **Exposure time:** The amount of time the hazard exists.
- **Number of exposed aircraft:** Number of aircraft exposed to the hazards.

Effects and exposure are considered at this stage of the framework rather than post-recovery, since at this stage there may be *potential* for significant consequences on safety, and one or several of the above will be impacted by the disturbance, even prior to recovery.

2.5.3 Interview findings

The relevance of these issues of effects and exposure was confirmed in the interviews. In terms of effects on the air navigation service, certain failures and associated disturbances would cause a serious inability to provide or maintain a safe service, significantly increasing workload and stress such that controllers are unable to perform their tasks effectively, with a large reduction of the ability to cope with other adverse operational and environmental conditions (e.g. total loss of R/T; total loss of radar). In such cases capacity would be seriously affected. Other failures would permit the ability to provide safe but degraded service, affect workload, stress or working conditions such that controllers' abilities are slightly impaired, and slightly reduce the ability of controllers to cope with adverse operational and environmental conditions (e.g. single workstation failure; flight data processing problems). One controller stated that, if a conflict or operational problem occurred simultaneously with a technical failure, it was particularly difficult to maintain awareness of the total situation and easy to neglect routine traffic.

In terms of exposure certain failures may be present for a substantial period of time, and reduction of safety margins may persist even after recovering from the immediate problem. One centre experienced a failure of a computer within the Radar Data Processing (RDP) system, which resulted in a total loss of radar services for hundred seconds in the early hours of the morning. However, in this case, there was no impact on ATC service delivery, no flow control was applied and no ATC incident reports were filed. The exposure time of other failures may be such that no significant consequences are expected (e.g. flight progress strip printing problems). Single radar failures can persist for some time, as engineers may have to visit a remote radar site.

Another centre reported the loss of sixty communication lines (data and communication), resulting in the loss of landlines to airports and backup R/T frequencies. Fortunately, traffic load was low at the time. The event lasted six to eight hours from loss to recovery. Controllers did not have direct dial telephone numbers for airports to hand, because the numbers were (previously) 'quick dials' programmed into the telephones; this information needed to be given out by supervisors.

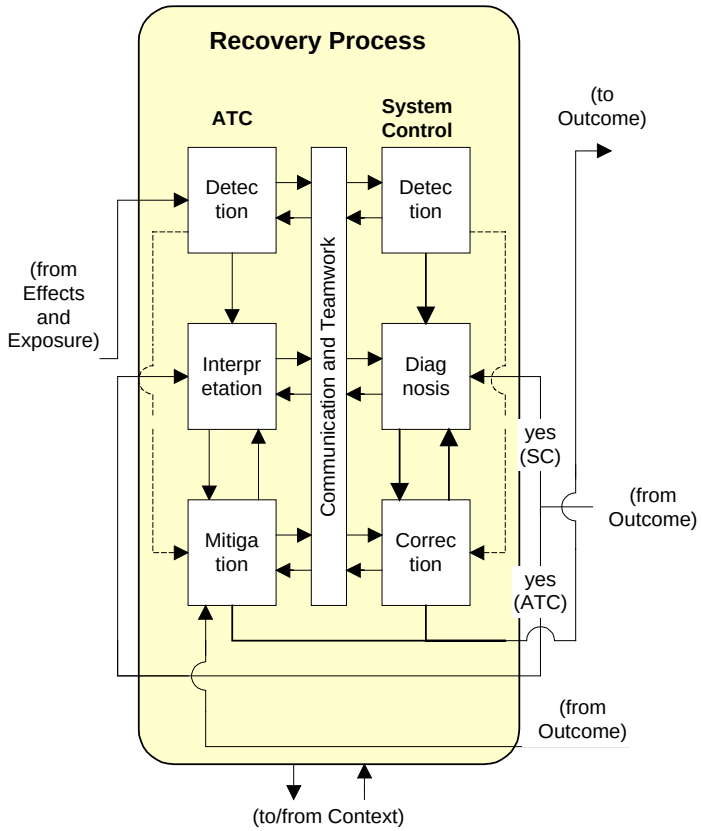
In other cases, failures may not be present for long. The severity of a failure to receive FDP data depends very much on the duration of the loss of FDP

information. In many instances the system automatically restores itself in less than a minute, then a partial download of all information that should have been transferred takes place. In such a situation system control advises ATC and later declares that the recovery is complete. If all this occurs within three minutes there will be minimal impact on the controllers, as electronic coordination, etc. is still possible.

Many of the failures described above will affect all aircraft in the area of responsibility (total loss of RT, total loss of radar, loss of SSR, etc.), while others may affect just one or two aircraft (e.g. code-callsign and squawk problems, ghost tracks, flight progress strip printing problems).

The effects on the air navigation service of a function disturbance may range from no effect or a slight effect, to a total inability to provide a safe service, with total loss of functional capabilities, a loss of ability to cope with other adverse operational and environmental conditions, causing high workload and stress for the controllers and flight crew affected. The exposure may range from a very brief exposure time, or persisting for only a short period, with no or only one aircraft affected, to the permanent presence of the hazard and persistent reduction of safety margins, affecting all aircraft in an area of responsibility.

2.6 Recovery Process



The next aspect of the RAFT Framework is central to this recovery-oriented approach – the recovery process. The following sections will attempt to take a closer look at the literature on the impact of automation on factors affecting the management of disturbances. This will consider research conducted both within and outside ATM (e.g. cockpit automation and pilot performance). The framework presented in Section 2.1 will be used to guide the discussion on the current literature reviewed.

The EUROCONTROL Air Navigation Service SAM states that in some cases it may be possible to evaluate a potential recovery process, following the likely chronological order of the steps involved: detection, diagnosis, annunciation and implementation of contingency measures. The guidance recommends that the following be considered:

- **Annunciation, detection and diagnosis:** Relevant factors are clarity of annunciation/indication, ease of detection and likelihood of correct diagnosis.

- **Contingency measures:** In some cases it may be also possible to consider the availability of alternative procedures, fallback equipment and ability to apply contingency measures within the scope of procedures and training.

- **Rate of development of the hazardous condition:** Rate of development of the hazardous condition (e.g. sudden, moderate, slow) compared to the average time required for recovering from unsafe conditions.

It can be seen that these correlate closely to the recovery stages in the RAFT Framework. These stages will be discussed in the following sub-sections, with illustrative findings from the research literature.

2.6.1 Detection

The first stage of the error recovery process involves 'detection' (Kontogiannis, 1999; Kanse and van der Schaaf, 2000) – realising or suspecting that a disturbance is about to occur or has occurred. This stage involves perceptual and memory processes that interact with the controller's or engineer's mental model of the system. The engineer or controller may have previous experience of the same or a similar disturbance (e.g. in training or operations or discussions with colleagues). Alternatively, the engineer or controller may be experiencing the problem for the first time, but detect that the system behaviour has transgressed the boundaries of 'normal operations'. At this stage of the recovery process, however, the controller or engineer has not diagnosed or localised the nature and cause of the disturbance.

Disturbances may be transparent (obvious) or opaque (hidden), on a 'data-driven', physical level (i.e. display properties or surface level features) or on a 'resource-dependent', cognitive level (i.e. due to characteristics of the human information processing system). A clearly displayed alert may remain undetected if the controller is very preoccupied, fatigued, or overloaded. On the other hand, an alert which is barely visible or audible may remain undetected even to a highly alert and motivated controller. More often though, data qualities and mental resources will combine to determine the likelihood of successful detection.

Disturbances may be detected by one or more people, either controllers (e.g. by noticing from the display) or engineers (e.g. by receiving an alarm). Disturbances may be minor or critical and may be detected before they have any adverse effects (e.g. detection of an alarm prior to any impact on controller workload or traffic handling) or after they have had an adverse effect (e.g. total loss of availability of a critical function). The following sub-sections deal with some of the main issues relating to detection of automation failures and disturbances.

2.6.1.1 Monitoring and component proliferation

By automating those tasks which can easily and effectively be automated, the remaining tasks are those that the human is least well-equipped to perform. One of these tasks is monitoring. Bainbridge (1987) termed this one of the *ironies of automation*. Parasuraman (1987) confirmed that humans do not make very good monitors. Wickens (1992) states that it may seem intuitive to automate the monitoring function as well, but this simply adds more components, all of which are subject to failure and yet distance the human yet further from the process under his or her responsibility.

Wickens (1992) states that when any single function is automated it usually increases by at least three the number of 'things' that must be monitored and could fail – the function itself, the health of the automated device designed to accomplish that function and the indicator of that health. Put another way, there may be failures of the initial system (like the aircraft engine), or of the automated device that controls the system (like the autopilot) or of the

supervisory monitor that monitors the health of both these systems. Furthermore, the monitor could either fail to indicate a malfunction in the systems that it monitors (a 'miss'), or it could incorrectly signal a failure in a healthy system (a 'false alarm'). Both have negative knock-on effects on human monitoring performance. The proliferation of components increases the likelihood that something, somewhere in the system, will fail. Wickens (1992) states that the likelihood of one thing failing is equal to one minus the product of the reliability of all components. Since component reliabilities are less than one, the product will decrease as more components are added.

The correct behaviour of the process may in fact be difficult to determine unambiguously. Another problem is that computers can operate much more quickly than a human where decisions can be fully specified, again, making it difficult for the person to monitor the correctness of decisions. Hence, the human is given an impossible task and can at best only monitor whether decisions are acceptable. But where the human disagrees with the computer-generated decision, who has the final say?

The human is always required at some level to monitor the automation – a task that humans are not well-equipped to perform. Automation tends to increase the number of components that need to be monitored, and may perform faster or in a more complex way than humans, and so making the task even more difficult.

2.6.1.2 Complacency and over-trust

Much of the automation or cognitive support that has already been implemented supports three information processing functions: *information extraction* (directing attention and aiding the selection of information), *information integration* (grouping or organising information) and basic *information comprehension* (adding meaning and pertinence). There is much evidence pointing to the value of such automation (MacMillan *et al.*, 1997, Parasuraman *et al.*, 1993). Wickens (1999) recommended that high levels of automation be pursued for these functions, *as long as the processes are reliable*.

Wickens (1992) cites laboratory evidence for the reduced accuracy of failure detection in automated processes. In various experiments cited by Wickens (Bortolousse and Vidulich, 1989; Ephrath and Young, 1981; Kessel and Wickens, 1982; Wickens and Kessel, 1979, 1980; and Young, 1969), operators engaged in laboratory tracking tasks or more realistic flight simulators were required to detect changes in the dynamics of a tracking system that was either controlled manually by the operator or by an autopilot. Operators were consistently slower and less accurate in failure detection when they were out of the loop.

Yeh *et al.* (1998) studied an attention-cueing tool for army threat target recognition. They found that when the cueing facility was present, detection of

cued targets was better than without cueing facility. However, they also found that the probability of missing targets not cued was higher when the cueing facility was available. Conejo and Wickens (1997) investigated target cueing or highlighting in a simulated air-ground targeting task. It was found that when the cue was unreliable (i.e. it directed attention to something that was not the designated target), pilots were still very likely to choose this non-target as the target, despite the fact that true target position and identity known to pilot was directly visible on the display.

Wickens (1999) stated that there is often a dependency on automated cueing, so that people can miss non-cued targets of greater priority and danger. Also, when cueing is unreliable, humans can choose 'non-targets', even when the true targets are clearly visible on the display.

These findings highlight issues of passive monitoring and miscalibrated *trust* in automation. Muir (1988) (cited in Wickens, 1992) stated that humans do not show optimally calibrated trust in automaton, i.e. trust which correlates with the reliability of a machine. Instead they shift from complete trust, to complete distrust once an automated device has shown itself to be fallible[4]. Trust is only regained slowly with repeated failure-free operation (Moray and Lee, 1990 [cited in Wickens, 1992]).

With excessive trust operators can begin to over-rely on the automation, leading to *complacency* (Weiner, 1981; Bainbridge, 1983; Parasuraman *et al.*, 1993; Singh *et al.*, 1993; Parasuraman and Riley, 1997). Complacency then further increases the likelihood of failure to monitor the state of the automated system and inputs into the system.

Parasuraman *et al.* (1993) proposed that performance benefits from high level automation of decision-making trade-off with performance decrements associated with complacency. The human becomes less likely to detect failures in the automation or processes controlled by the automation. Wickens (1999) also states that with the use of high level automation for decision-making, humans become less likely to detect failures in the automation itself, or in the process controlled by the automation, if they were only passively observing the automation.

Analyses of Aviation Safety Reporting System (ASRS) reports have provided evidence of monitoring failures linked to over-reliance on automated systems such as autopilot and Flight Management System (FMS) (Singh *et al*., 1993). The ASRS coding manual defined complacency as self satisfaction which may result in non-vigilance based on an unjustified assumption of satisfactory system, state (Billings *et al*., 1976). Wiener (1981) searched the ASRS database and found over five hundred incidents of complacency that could be attributed to crew over-reliance on automated systems. Mosier *et al*. (1994) found 77% of incidents were suspected over-reliance on automation and involved probable failure in monitoring.

[4] See EATM (2003a, b, c) for a more complete discussion on trust.

These phenomena are often referred to as the syndrome '*out of the loop unfamiliarity*'. Bainbridge (1983) notes that the more reliable the automation, the more susceptible to 'out of the loop unfamiliarity' the operator will be if a failure does occur, largely because of increased complacency. The human is placed in a monotonous situation and yet expected to maintain situation awareness react appropriately to problems. Assuming a person is 'in-the-loop', Wickens (1992) again suggests an inverse relationship between equipment reliability (or rather perceived equipment reliability) and human reliability. Wickens states that 'It is likely…that the operator will become far more cautious, trustworthy, and reliable when interacting with a system that has a higher likelihood of failure or with a component that itself has just failed than when interacting with a system that is assumed to be infallible.' (p. 433). If this were true, it would place system designers in a double-bind situation.

It seems that *the more reliable, predictable and dependable a system is, the more trust and hence more complacency develops*. Indeed, May *et al*. (1993) found an inverse relationship between automation reliability and automation failure detection performance, when examining a range of reliabilities from 12% to 98%. This would add a serious caveat to Wickens (1999) recommendation that high levels of automation be pursued for basic information processing functions; a *very high* level of reliability would be required. In a follow-on study to May *et al*. (1993), Parasuraman *et al.* (1993) used the same monitoring task in a single task environment. When engine monitoring was the *only* task (a situation that is unrealistic), detection was equally reliable during manual control as it was under automated control.

Parasuraman *et al.* (1993) tested non-pilot participants on a laboratory flight-simulation task consisting of three tasks; a two-dimensional compensatory tracking, a probability monitoring task of engine status, and a fuel management. In a multi-task condition participants were required to perform the tracking and fuel management tasks manually while an automation routine detected engine malfunctions. This automation routine failed intermittently and participants were required to detect the fault. Participant groups were exposed to different failure rates, which were either constant or variable. It was found that detection of engine malfunctions was significantly worse for the automated engine status monitoring condition when compared to the manual engine status task. Failure detection performance was not related to the mean level of automation reliability, but was associated with the variability in automation reliability. The probability of detection of automation failure was 60% lower when automation reliability was constant compared to when automation reliability varied over time.

With increasing levels of automation people tend to become more 'out of the loop', and so less able to spot occasional and difficult-to-detect disturbances. Further, the more reliable, predictable and dependable a system is, the more trust and complacency develops. But humans do not show optimally calibrated trust in automaton, i.e. trust which correlates with the reliability of a machine. Instead they tend to shift from complete trust in seemingly reliable automated devices, to complete distrust once the device has shown itself to be fallible.

2.6.1.3 Situation awareness

Another related perspective on the issue of detecting system disturbances is that of Situation Awareness (SA). Garland and Hopkin (1994) suggest that automation can influence the controller's SA. High levels of automation endanger SA in four respects:

1. SA may degrade if automation accomplishes operations and fails to inform operators of these operations or changes.

2. Automation-induced complacency may reduce levels of vigilance and so state changes may not be noticed.

3. People are more likely to remember state changes if they have been active agents rather than passive witnesses (Hopkin 1995; Vortac, 1993).

4. An accurate and updated mental model of the ATM system is needed for effective maintenance of SA, especially if 'mental models' of the system developed in automated mode do not transfer to performance in manual mode (Kessel and Wickens, 1982).

Sarter and Woods (1995) propose that, if automation was designed to carry out functions in a different and more complex way, then the humans would normally carry out the task, the human operator might be less able to encode and remember state changes. It stands to reason that if automation represents information in a manner that is too complex for humans to understand, then humans cannot be expected to maintain situation awareness.

Wickens *et al.* (1997) suggest that if controllers accept the presence of conflicts and proposed solutions as a matter of routine, a loss in SA may develop compared to when conflicts are detected manually and solutions are generated manually. Whitfield *et al.* (1980) reported a loss of mental picture in Air Traffic Controllers (ATCOs) who tended to use automated resolutions under conditions of high workload and time pressure.

There is plenty of evidence for the loss of SA effect. Wempe (1965) found pilots were unaware of autopilot disconnects. Bergeron (1981) found that pilots working in increased level of automation were more likely to lose track of

where they were. Endsley and Kiris (1995) implemented automation of an automobile navigation task (through an expert system) at five levels of automation, from fully manual to fully automatic. They found that the out-of-the-loop performance problem was greater, and SA was lower, under full automation than under intermediate automation. It was also found that subjects who were not required to work through the problems as the expert system provided the solutions had decreased 'level 2 SA' – related to comprehension of meaning – and concluded that subjects did not develop the higher level understanding of a situation. This level of SA is crucial for effective problem detection, diagnosis and control. At lower levels of SA, where operators were still involved in decision-making, SA remained higher and operators were more able to perform the task manually when required, such as during automation failure. Endsley and Kiris concluded that loss in SA is attributable to lack of active information processing and the need to shift from passive information processing to active information processing when automation fails. Similarly, Carmody and Gluckman (1993) found level 2 SA (but not level 1 – related to perception of elements in the environment within a volume of time and space) was lower under fully automated conditions.

The reason for reduced SA may be that passive processing of information leads to less effective integration and dynamic update of information in working memory when compared to active processing of information (Cowan, 1988; Slamecka and Graf, 1978).

Out-of-the-loop performance has been attributed to loss of operator SA (Endsley, 1987, Carmody and Gluckman, 1993), as well as vigilance decrements and complacency (Wiener, 1988; Parasuraman *et al*., 1993), poor feedback under automated conditions (Norman, 1990) and manual skill decay (Wiener and Curry, 1980). Endsley (1987) hypothesised that a loss of SA underlies a great part of the out-of-the-loop performance decrement. Human operators lose SA and may be slower to detect problems as extra time is required to reorient themselves to relevant system parameters in order to proceed with problem diagnosis and manual performance. However, findings have been inconclusive about the relationship between out-of-the-loop performance and SA. It is unclear if the relationship is causal and what is the direction of the relationship.

Some studies have provided evidence of the benefits on SA of automation which assists information integration and response implementation, such as datalink (Endsley and Smolensky, 1998; Endsley and Kiris, 1995), but many other claims are not sufficiently substantiated. Wiener (1992) (cited in Endsley and Kiris, 1995) suggests that SA may be enhanced with automated systems which can provide superior integrated information to operators. Billings (1991) proposed that automation provides pilots with better integrated information and thus allows them to manage at higher workload levels. However, on the contrary, Bainbridge (1983) noted that when workload is highest, automation is often of the least assistance as it can usually handle only routine tasks. Also, Endsley (1993) demonstrated a degree of independence between SA and workload. This means that, even if workload is successfully reduced, this may not translate into higher SA.

An important caveat to the research findings is that researchers use varied and diverse methodologies and definitions, especially in the definition of the levels of automation, ranges used and the tasks performed by humans. However, overall the evidence suggests that automation often reduces SA. Reduced SA – particularly level 1 SA – will clearly have an impact on the ability to detect system failures.

Low and Donohoe (2001) performed a rare study of recovery from failure in ATM. The failures simulated were total radar failure and Secondary Surveillance Radar (SSR) code failure (where aircraft callsign and height readout information is lost from the radar display). The study was conducted over three days on two London terminal control sectors. Emergency training exercises were used, each with a medium to high traffic loading. The key methods used to assess recovery performance were Eye Movement Tracking (EMT) and the Situation Awareness Global Assessment Technique (SAGAT). EMT revealed that visual search was slower when the SSR failure occurred. Scanning behaviour suggested a 'tunnelling' effect; visual attention was focussed around Heathrow and Gatwick with little or no attention paid to other areas. Interestingly, following radar failure, visual scans similar to those before the failure were still observed on the blank radar display, though this effect dissipated as time progressed. When SSR returned, controllers searched more and faster than before the failure, though there was no such difference when radar returned. The measurement of SA showed that SA decreased as the failure period progressed. This was due to the less accurate awareness of geographical aircraft locations, rather than a decrease in other traffic information.

On a more positive note, Endsley and Smolensky (1998) state that some implementations of automation may provide as many opportunities for SA improvements as they do for SA decrements, and that finding the types of automation that may aid SA, as opposed to compromising it, is the greatest single challenge of the automation age.

High levels of automation endanger situation awareness if:

- **feedback is poor,**
- **automation-induced complacency occurs,**
- **people are passive and out of the loop,**
- **the automation performs in complex way, and**
- **'mental models' of the system developed in automated mode do not transfer to performance in manual mode.**

Automation design must overcome these issues in order to maintain an appropriate level of SA required for managing system disturbances.

2.6.1.4 Underload and vigilance decrements

Underload can have destructive effects on human performance (Bainbridge, 1983; Wickens *et al*. 1997) and yet this is a relatively neglected in Human

Factors (HF) research in ATC (Hopkin, 1995). Underload may be a particular problem when the human role is reduced to monitoring rare and low salience events, such as system disturbances. Underload can be explained in terms of vigilance decrements. Vigilance has been defined as 'a state of readiness to detect and respond to certain small changes occurring at random time intervals in the environment' (Mackworth, 1957, pp. 389-390).

The decline in detection performance over time in such conditions is well established (Davies and Parasuraman, 1982); people detect fewer targets and take longer to respond to targets. This decrement typically occurs within thirty minutes (Teichner, 1974), or as little as five minutes for perceptually demanding targets (Nuechterlein *et al*., 1983). In general, vigilance is high for targets that are highly salient, temporally and spatially predictable, and occur frequently in the context of a low background event rate[5]. However, adverse events related to automation rarely display these characteristics. Signal detection theory suggests two possible sources of vigilance decrement: a decrement in perceptual sensitivity (d) and an increment in response bias (b) over time. Roughly, this means that people become less able to detect targets and less willing to call a target an event. There is evidence to suggest that these adverse effects can be reduced with training (Bisseret, 1981; Davies and Parasuraman, 1982; Craig, 1985).

Although maintaining vigilance can be boring, it actually imposes high levels of mental workload (Wickens *et al.*, 1997). Warm *et al.* (1996) found that even trivial vigilance tasks impose a level of subjective mental workload equivalent to tasks involving problem solving and decision-making, and are subject to various performance-influencing factors. Warm *et al*. used a simulated air traffic control display which provided advance notification of a conflict. This reduced rather than increased subjective workload, even though this should increase boredom because the operator is left with little to do. It was concluded that the workload was directly task-related and was not a by-product of boredom.

➘ Example – Failure to detect an automated system failure 1
A PAA B-707 experienced a graceful autopilot disconnect while cruising at 36,000 feet above the Atlantic. The aircraft went into a steep descending spiral loosing 30,000 feet before the crew recovered the situation (Wiener and Curry, 1980).

➘ Example – Failure to detect an automated system failure 2
An Eastern Air Lines L-1011 slowly flew into the Florida Everglades after an autopilot became disengaged. The crew and ATC failed to notice the autopilot disengagement.

[5] This general principle regarding predictability conflicts with the finding of Parasuraman *et al.* (1993), who found that the probability of detection of automation failure was 60% lower when automation reliability was constant compared to when automation reliability varied over time.

Low traffic load has been associated with operating irregularities (Stager *et al*., 1989). The Canadian Aviation Safety Board (1990) found that of 217 incidents selected from 437 occurrences, 60% of the system errors were attributed to planning judgement or attention lapses on the part of the controller. However, most of the operational errors occurred during conditions of low traffic complexity. Rodgers (1993) found similar results for US controllers.

Currently, ATC automation has primarily replaced some of the routine data processing tasks that controllers previously performed (information extraction and integration). Wickens (1999) argues that this low level form of automation may not harm controller vigilance. However, there is evidence that detection of critical events is affected by vigilance. Thackray and Touchstone (1989) performed an experiment where student participants performed a simulated ATC task. The task involved detecting one of three types of critical event: (1) a change in the altitude part of the data block to 'XXX', simulating a transponder malfunction; and two aircraft at the same altitude and either moving (2) toward each other (conflict) or (3) away from each other (non-conflict) on the same flight path. Nine critical events were presented during each thirty-minute segment of a two-hour vigil. While subjects detected all of the transponder malfunction targets and showed little change in speed of detection over time on task, for the same-altitude targets, a vigilance decrement over time was observed, both in the number of targets detected and in the speed of detection. Since the latter task imposed greater processing demand, the findings suggest that the information processing demands increased the likelihood of a vigilance failure occurring during extended watches.

Wickens *et al*. (1997) state that the emphasis on detection vigilance may not be so relevant in light of ATM sensory technology, but the vigilance problem may have shifted to the area of discrimination, recognition and diagnosis of unusual conditions.

When 'underloaded', people tend to detect fewer targets and take longer to respond to targets, within a short time. People may also be less able to discriminate, recognise and diagnose unusual conditions. Although maintaining vigilance can be boring, it actually imposes high levels of mental workload.

2.6.1.5 Task load

Studies of the effect of task load on failure detection have been mixed. Thackray and Touchstone (1989) designed an experiment to validate empirically the concept of complacency on an ATC monitoring task. Student participants performed a simulated ATC monitoring task using a console closely resembling a radar workstation, either with or without an automated aid message indicating aircraft-to-aircraft conflict situations. The automation failed on two occasions, early and late, during a two-hour session. Thackray and Touchstone hypothesised that participants would be less efficient in detecting ATC conflicts with automated aids than without automated aids, but found that

participants detected ATC conflicts equally well in both conditions, thus finding no evidence of complacency. However, other studies suggest that overall task load influences the monitoring of automation (Parasuraman, 1987; Parasuraman *et al*., 1993, 1994). Indeed, Parasuraman *et al*. (1993, 1994) found that monitoring of failures in the automated control of a task is poorer than manual monitoring when operators are engaged simultaneously in other tasks. When monitoring was the only task, operators were usually very efficient at detecting any failures in automation. However, the monitoring of automation failures is degraded when operators have to carry out another task simultaneously. They also found that if the system is more inconsistent, operators were better at monitoring automation failures. Hence, they suggest that complacency appears to have an effect on monitoring performance when task load is high and if the system is reliable. Singh *et al.* (1997) also argued that the reason for Thackray and Touchstone's (1989) findings was that the subjects had just one task to perform (monitoring). This situation is rare in ATM, and in the cockpit where many monitoring failures occur when the pilot is multitasking (e.g. monitoring, data entry and communications).

Wickens *et al.* (1997) note that two opposing predictions can be made: 1) that vigilance failures might be exacerbated with the additional demands imposed by other activities, which decrease available resources and increase the information processing demands of target detection (Parasuraman *et al*. (1994); and 2) task load should improve vigilance performance since boredom is reduced (Sawin and Scerbo, 1994). Currently there is no definitive answer.

2.6.1.6 Display location

Another relevant issue is eye-movements and display location (sometimes referred to as the 'out-of-sight bias' - See EATMP, 2002, 2003f). In some previous studies the automation task was located in the periphery of the display space. Hence, Singh *et al.* (1997) studied whether centrally locating an automated system monitoring task would boost performance of a flight-simulation task consisting of system monitoring, tracking and fuel resource management subtasks. Twelve non-pilot participants performed the tracking and fuel management task manually while watching the automated system monitoring task for occasional failures. The automation reliability was constant for six participants and variable for the other six participants. In each automation reliability condition the automation routine was disabled for the last twenty minutes of the last session in order to simulate catastrophic automation failure.

The study found that monitoring performance under automation was inferior to performance of the same task under manual conditions and confirmed Parasuraman *et al*.'s findings (1993) that monitoring in a constant-reliability condition is worse that monitoring a variable reliability condition. However, centrally locating the monitoring display had no significant effect. Singh *et al.* (1997) concluded that automation-induced monitoring failures cannot be prevented by centrally locating the automated task and that the 'automation complacency' effect is a relatively robust phenomenon. Singh *et al.* offer an explanation in terms of attention resource allocation to the monitoring of

automation. However, neither tracking nor fuel-management performance differed as a function of automation reliability, suggesting that differential allocation of processing resources cannot account for the superiority of monitoring performance in the variable reliability condition. Trust may also have been an important factor. As reliability fluctuated for the variable group, trust may have declined, leading to scepticism and increased vigilance.

It appears that centrally locating an automation-related display does not significantly improve the detection of disturbances.

2.6.1.7 Interview findings

There seem to be several ways in which failures and disturbances were detected in the three centres. These can be summarised as follows:

- visual feedback indicating the failure,
- automatic switching to a fallback mode,
- total loss of the function (which may either be obvious or difficult to detect),
- timing problems,
- corruption of data,
- suspicion of a problem and
- fault reporting from system control.

Often a combination of these methods will announce a given failure. Considering the first of these, in some cases (often with serious system problems) where there is clear feedback, ATC detection of system disturbances is relatively easy. For instance, one centre announces problems using a brown border, together with a text message giving brief information on the failure. Major failures are also announced by a yellow cross overlaid onto this display. For example, STCA and track shedding due to overloading of Single or Multi-radar Processing (SRP/MRP), or loss of MRP results in a frozen radar picture and a yellow cross appears over the radar display for all tactical and planner controllers in one of the centres visited. In another, loss of MRP produces the message ‘antenna off’ in a window on the radar display. In this centre, the quality of radar track is indicated in shape and colour of aircraft target.

In other cases ATC may be made aware of a problem by a (less clear) visual message. When controllers at one centre lost Flight Plan Processing (FPP) functionality, the system blocked data and automatic coordination was not possible. The problem was detected by ATC when controllers saw a message in a window on the radar display to coordinate manually. However, at the same time an engineering alarm was raised and the watch supervisor received information from system control.

In the case of single workstation failures some centres reported that the fallback mode automatically activates. This again presents clear feedback, and has fewer or different functions and a different display.

Other failures result in a total loss of function, without complementary feedback. For instance, on the loss of R/T (input, output or both), or perhaps loss of telephone communications, often no indication is provided to controllers other than the loss of the function, which will be noticed on attempting to communicate. If an individual keyboard or mouse fails, the controller will be unable to interact with aircraft track data blocks, electronic strips and other functions on radar. This again will be obvious as soon as the control tries to use the function.

Timing problems may be quite difficult to detect in some cases, at least initially. Controllers at one centre reported receiving flight progress strips late. Others reported late automatic coordination requests. Such problems may therefore be difficult to detect at first, until the controller suspects that a problem has occurred. Another timing problem reported at another centre was an increase in individual workstation response times. The controller notices slowed updates or responses to radar functions. The volume of interest (the geographic area within which aircraft tracks will be displayed) may shrink as shedding of tracks occurs.

Data corruption will often be easy to detect. An individual radar display may become distorted (colour, focus or clarity problems), or unreadable text and/or graphics may appear on the radar display. Interviewees at one centre reported a problem with graphics cards causing problems in the display of text. Interference on an individual R/T frequency will also be easily detectable, as controller or pilots, or both, may not be able to hear all messages clearly.

Other problems are not so obvious. These generally involve problems with data integrity. The controller may suspect that data has low integrity. In the case of the appearance of ‘ghost tracks’ on radar displays, (i.e. two aircraft with same track data block details), controllers will usually be aware which is the actual aircraft, but an element of doubt will exist. Similarly, a problem may occur where the Mode C height readout does not reflect the actual altitude of the aircraft (e.g. ‘jittering’ by $\pm$ 500ft). Detection of such a problem may not be reliable, and upon detection the controller will be unsure about actual altitude of the aircraft. However, system control may detect this problem via the control and monitoring system. A third example is the code-callsign conversion error, where aircraft track data blocks are transposed between two aircraft within a sector. This can be very difficult to detect and may only be detected upon an instruction intended for one aircraft *seemingly* being taken up by another. The controller will be uncertain about the aircraft position and behaviour.

On the whole the majority of failures (but not all, e.g. ghost tracks and mouse or keyboard failures) will be detected in parallel by system control staff, who receive alarms for most types of failure via the control and monitoring system.

Multiple, clear and timely means of detection should be available to alert controllers and engineers to disturbances and failures. Controllers and engineers should not have to detect an absence of feedback, or subtle changes in information. An indication of the integrity of performance, information, etc, should be available if possible.

2.6.2 Interpretation and diagnosis

The next stages of the recovery process are interpretation (ATC) and diagnosis (system control). The controller interprets and assesses the functional disturbance to determine what is occurring, the level of risk imposed, whether the function is still dependable and what else might be affected. The engineer diagnoses the causes of the failure and any related problem that have or may have occurred. Some disturbances will be more difficult to diagnose, particularly if they are complex (e.g. several causes) or unfamiliar. The RAFT Framework is flexible with regard to the interpretation/ diagnosis and mitigation/correction phases. Accident and near-miss data shows that the sequence of the phases varies (Kanse and van der Schaaf, 2000). The interpretation/diagnosis phase may not occur immediately after detection of a problem, but instead after or in parallel with initial mitigation and correction.

This stage of the recovery process will be different for controllers and system engineers. The controller performs interprets the situation differently to the system engineer. For instance, with automation of information integration functions, the controller is concerned about data quality, including missing data, corruption and loss of integrity. The controller therefore has to make a decision about the quality of the data and whether it should be used. If data is not reliable, then the controller will disregard it and pass the problem to the system engineer. It may be that *the controller engages in interpretation activities only to the extent that the controller perceives that he or she can correct the problem*. For instance, if there is a problem with radar data or electronic coordination, then the controller may change radars or perform manual coordination. However, where a controller is not able to correct a problem, once the problem is detected, the controller will not become involved in further detailed interpretation or diagnosis – this is the job of the system engineer.

Lees (1980) describes different ways of diagnosing system disturbances. For frequent or well-known faults, a person may simply respond to the first alarm generated, where the alarm is associated with a particular fault and a particular rule of thumb is adopted. Another strategy is to apply pattern recognition to the control panel displays. This may be static pattern recognition, taking a snapshot of the situation and matching this to a stored pattern, or dynamic pattern recognition over time. A third strategy is to use a ‘mental decision tree’, perhaps using a series of ‘if-then’ rules. Finally, the person may manipulate elements of the system to observe the effect. An

engineer may revert to a previous software version to check if a bug still exists. A controller may ask a pilot to 'squawk ident.' in a situation involving code-callsign confusion.

Complex diagnosis will not always be necessary. For example, frequently experienced disturbances will have familiar symptoms. However, a problem could arise if different problems have similar symptoms, thus lulling the controller or engineer into a false sense of security. Diagnosis will also depend on the time available. In time-pressured situations controllers or engineers may attempt an initial and rapid corrective action without performing a full diagnosis.

While the controller interprets the implications of the functional disturbance on the control task, the engineer attempts to diagnose the cause of the technical failure. There are several ways of diagnosing a problem, from simple rule of thumb approaches for known problems, pattern recognition and if-then rules to manual manipulation of the system. Such problem solving activity may pull the team together.

At the stage of diagnosis more team interaction can be observed. Kanse and van der Schaaf (2000) found that diagnosis tends to have the effect of bringing team members together, finding that often more people participated in this phase of recovery (mostly colleagues from the same operating team).

Wickens (1992) states that the proliferation of components and the associated increase in system complexity will magnify the problems associated with fault diagnosis. According to Wickens *et al*. (1997), while automation enhancements may be transparent to controllers, they can impose a requirement to learn new and complex functional and human-machine characteristics of the modernised equipment. Similarly, Leveson (1995) states that computers often overload human operators with information, as is the case with 'alarm flooding', where hundreds of poorly prioritised alarms can appear following a failure. In such situations, people tend to take no action until they have a better understanding of the situation, by which time it may be too late. Even where information is minimised, problems still occur. Humans are naturally inquisitive and operators will tend to manipulate the system, or experiment to get the information they need to form an adequate mental model of the system (Note: A mental model is a 'mechanism whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future states' [Rouse and Morris, 1985, p. 7].) This activity may approach random or panicky behaviour at times and many lead to failures. Alternatively, it may reveal information that could produce 'insight learning' to deal with a failure, or help deal with previously unanticipated situations.

➘ Example – Alarm flooding 1
During the Three Mile Island Accident, so many alarms had to be printed that the printer fell behind by as much as two hours in recording them.

➘ Example – Alarm flooding 2
During the Bhopal Accident, indications of a problem were not taken seriously because so many previous alarms had been spurious.

Shorrock *et al*. (2002) state that the burgeoning use of 'soft-desk' alarm systems employing Visual Display Unit (VDU) technology, instead of hard-wired alarm systems, has resulted in various problems in alarm handling. Alarm systems represent one of the most essential and important interfaces between human operators and safety-critical processes, yet often one of the most problematic. Engineering psychology has paid considerable attention to the design of alarm systems, particularly in the process industries. This has been spurred by several major accident investigations, including Three Mile Island (1979), Milford Haven refinery in the UK (1994) and the Channel Tunnel (1996). In the UK investigations by the Department of Trade and Industry and Health and Safety Executive (2000) have found significant HF deficiencies in alarm handling. Alarm flooding, poorly prioritised alarms and 'clumsy automation' has prevented operators from detecting important alarms, understanding the system state, and reacting in a directed and timely manner. Indeed, poorly designed alarm systems can hinder rather than help the operator (Swann, 1999). One cause of this problem is that control rooms are migrating many alarms to a limited display space without an adequate 'alarm philosophy' (Shorrock *et al*., 2002).

Alarm flooding occurs when too many, poorly prioritised alarms appear following a problem than the person can deal with effectively. In such cases, people may not take action when required because they are trying to update their mental model, or they may take the wrong action, for instance due to time pressure or panic.

Brehmer (1987) states that the information received by an operator and the outcomes the operator creates are mediated by complex and opaque processes. Hence, operators have difficulties in forming mental models to help make decisions under conditions where they have little insight into the process they want to control. Indeed, Green (1990) (cited in Leveson, 1995) stated that pilots cannot possibly understand the technology involved in the generation of a display, so *they are compelled to use the display itself as their mental model if the world* instead of creating their own model from raw data. This behoves a great responsibility on designers to ensure that operators get the information they need to make good decisions. So depending on the operator's mental

model, system information or behaviour which indirectly indicates a malfunction may either be ignored (strong but wrong mental model) or not noticed (weak mental model).

Feedback from automated systems may be masked or delayed by designs that cause 'referred symptoms'; the place where a failure first becomes evident may not be where the failure has occurred.

➘ Example – How false alarms can influence behaviour
The crew of a Texas International DC-9 from Denver, when a stall warning spuriously activated occurred during take-off, aborted the take-off, in spite of normal airspeed and pitch attitude indications, resulting in runway overrun, severe damage and nonfatal injuries to passengers. The crew had experienced spurious stall warnings before, but had to choose between two potentially disastrous accidents (Wiener and Curry, 1980).

2.6.2.1 Effects of complacency and trust

Complacency and miscalibrated trust can affect diagnosis as well as detection performance. Wickens (1999) stated that humans may rely on diagnostic aids, even when such aids are unreliable and there is contradictory evidence. That is *humans may follow and believe unreliable automation even as the latter conflicts with clearly visible evidence*.

Mosier *et al*. (1998) provided partially reliable automated diagnostic aids to pilots and found that pilots trusted and followed advice even when the advice conflicted with directly visible and contradicting evidence. Similarly, Taylor *et al.* (1997) looked at combat scenarios and found that automated advice was followed even in the face of contradictory and visible evidence.

Venda and Lomov (1980) (cited in Leveson, 1995) showed that the likelihood of an operator talking over successfully when the automated system fails increases as the operator's subjective assessment of the probability of equipment failure increases.

2.6.2.2 Errors of diagnosis

Singleton (1989) describes some common phenomena in diagnostic errors. First, an operator may persist in pursuing an inappropriate hypothesis formed too hastily. Once formed, such a diagnosis directs the search for evidence, so that supportive data are readily accepted and non-supportive data are rejected (Perrow, 1984). This is variously referred to as 'confirmation bias', 'mind-set', or 'cognitive fixation'. Such errors of diagnosis are associated with a strong but wrong expectation about the situation, because of a faulty mental model which is resistant to change, and perhaps ambiguous information. Singleton states that this is probably less likely if the diagnostic process is shared between individuals and particularly if there is an independent monitor situated

elsewhere. This effect is intensified by the build-up of excessive trust in an automated system.

Second, there can be confusion between malfunction in the plant and malfunction in the information system reporting plant activity. Hence, malfunctions can occur at various levels, for instance at the level of aircraft and aircraft equipment, radars, RDP systems, networks, visual display units, etc.

Third, there can be misunderstanding between operators. In an ATC context this may be between air traffic controllers and system engineers. For instance, a system engineer may make an initial misdiagnosis based on the description provided by the controller, because the two specialists use different language and have different mental models of the system.

> **➘ Example – The 'confirmation bias'**
> In the Air New Zealand accident at Mount Erebus in Antarctica, the crew may have trusted the inertial navigation computers and were probably seduced into interpreting external visual information in a way that conformed with the world model generated for them by the aircraft' (Green 1990, cited in Leveson, 1995).

2.6.2.3 Interview findings

As previously mentioned, this stage differs for air traffic controller and system engineers. Generally speaking, operational controllers currently need to perform little interpretation because most failures are displayed fairly directly, either via supplementary feedback, loss of a function, obvious data corruption, etc. In other cases though, and probably more so in future, some interpretation is necessary. The most common types of failure requiring such interpretation involve a loss of data integrity or credible data corruption. An example of this can be seen in the code-callsign conversion error, where, after suspecting that there is a problem, the controller will have to work out which two aircraft are affected. With such problems it may take the controller some time to interpret the situation, and explain or localise the failure.

Controllers are only concerned about system performance when it becomes clear to them that their facilities are degraded. Whereas controllers may detect problems (e.g. a loss of their radar display), they do not see it as part of their function to diagnose or correct the problem. This is the role of system control personnel. For system control personnel diagnosis is assisted by the control and monitoring system. Such systems often provide 'mimics' or diagrammatic representations of ATC/CNS systems (see Shorrock and Scaife, 2001), which present hierarchical layers of icons, colour coded according to their integrity/availability. However, diagnosis may be very difficult when there are multiple failures.

2.6.3 Mitigation and correction

The third stage of the recovery process involves resolving the problem. This really entails two sub-processes: mitigation of the operational (ATC) impact and correction of the technical (engineering) problem. The first priority is clearly to minimise the effect on air navigation service and the exposure of the problem in terms of aircraft and time. This will require manual reversion, so that the (previously) automated function continues to be performed by the controller. For instance, if an automated conflict detection tool fails to work properly, then the controller must perform this function manually (once he or she has detected the problem, for instance by detecting a conflict that was not alerted automatically, then diagnosed that the conflict detection tool itself is not functioning properly). The timeframe for operational mitigation is short. Immediate or tactical action will often be required to ensure the safety of air traffic, while longer term strategic action such as flow control will also be necessary to reduce the impact of the problem. The second priority is to restore the availability of the correctly functioning automated function. This will normally be a longer term task, though it may be possible to bring systems back on-line in seconds or minutes.

In this stage of recovery both the controller and engineer will have to:

- reassess the problem in terms of the constraints set by system state, new developments and person's capabilities;
- decide on the goal of recovery;
- modify an existing plan or create new one to compensate; and
- execute in a timely fashion.

2.6.3.1 Manual reversion

Two of the key purposes of automation are to perform functions which either 1) the human operator cannot perform because of inherent human limitations (e.g. tasks involving complex data processing), or 2) the human operator can perform but does so slowly, poorly or at a cost of high workload (Wickens, 1992). This second function changes over time, as operating contexts and systems become more complex, as in the case of manual control of a modern wide-bodied aircraft, or the current method of ATC in a future environment of greatly increased traffic growth. If a function is automated because the human is ineffective at performing that function, it seems untenable to expect humans to be effective in reverting to manual performance following a system failure. Even now in ATC there are tasks that the controller no longer performs and have been replaced by technology such as SSR. A failure of such systems would cause great problems, even now, when the controller is in-the-loop and still very much in control of decision-making. Hopkin (1998) states that at present it may remain possible for a time for the controller to perform essential, safety-critical aspects of the ATC tasks, in the absence of current automation, though not to perform them efficiently.

The problem of manual reversion has been demonstrated in a number of industrial contexts.

Roske-Hofstrand and Murphy (1998) state that during a failure of SSR a highly disruptive problem is that aircraft without working transponders are not represented on the plan view display. In this situation controllers and pilots must cooperate completely to resolve the problem safely. Controllers have to devote more time to distinguish different aircraft, and transfers and handovers become more complex and time-consuming.

Brenlove (cited in Roske-Hofstrand and Murphy, 1998) states that 'a controller's primary concern is to establish non-radar separation standards. He or she will give little or no thought to the most direct or most efficient route for each aircraft. ATC instructions will be based entirely on the safest way to get the job done.' (p. 120). Hence, under degraded conditions the controller operates *only* to achieve the highest-level goal in ATC: safety.

Endsley and Kaber (1996) (cited in Endsley and Smolensky, 1998) conducted a study involving multiple goals, multiple tasks to be processed with different relevance to the assigned goals and high task demands under limited time resources, as would be found in ATC. The simulation required subjects to develop complex strategies for optimising system performance along multiple goals simultaneously. Various results were found for different levels of automation. However, it was found that time to recover and performance during manual control immediately following a failure were worse at levels of automation that incorporated advanced process planning.

Similarly, Endsley and Kaber (1999) found that the key factor in determining performance in the period immediately following an automation failure was the level of automation, in particular whether decision-making and response choice was automated. Of a number of levels of automation, time-to-recover from automation failure was highest in this latter mode. On the other hand, time-to-recover was lowest where the operator generated the options, chose an option and decided when to implement the option, and the system implemented the action. Implementation strategies that allowed for advanced process planning were the most disruptive. Implementation strategies that provided assistance to cope with manual workload while keeping the operator involved in decision-making operations appeared to be optimal.

The counterpart to manual reversion, which is rarely mentioned in the literature, is the return to the more automated mode when the system is functioning properly. Hopkin (1998) mentions that while continuing to perform the more limited but essential ATC functions of the manual mode, the controller may be unable to load into the repaired automated system all of the information required about the current traffic scenario, prior to returning to the automated mode. Hopkin predicted that the system may have to remain in the inefficient manual mode until the context permits the return to automation.

Manual reversion will only be possible if the human is capable of performing the safely task in the first place. The controller will usually attempt to achieve only the safety-related tasks. Time-to-recover will be greatest where higher levels of automation are implemented (e.g. decision-making and response choice). Automation that provides assistance to cope with manual workload while keeping the operator involved in decision-making operations appears to be optimal. The phase of return to automated mode also needs to be considered carefully in terms of workload and trust.

2.6.3.2 Loss of manual skills

One of the key factors affecting the correction of system disturbances is skill degradation and the loss of ability to perform tasks manually (Bainbridge, 1983; Parasuraman *et al.,* 1993; Wickens, 1999). This manual skill remains critically important as long as the potential remains to intervene in the case of a disturbance. High levels of automation, particularly where the decision-making functions are automated, provide very little opportunity to practise skills involved in performing tasks manually. The lack of practice may result in the degradation of manual skills and lead to an even greater reliance on automation (Lee and Moray, 1992; Satchell, 1993; Mosier *et al*., 1994). There is currently little or no objective evidence from field studies that prolonged use of automation is associated with decreases in manual performance for ATCOs. This is partly associated with the relatively low-level of automation currently in place. Also, such effects are difficult to demonstrate outside controlled settings, particularly in safety-critical work environments. However, there is evidence from other domains.

Shiff (1983) found that despite manual training, subjects who had been operating as supervisory controllers of automation in a simulated process control task were slower and more inefficient in bringing the system under control than were subjects who had operated only in a manual mode.

Weiner and Curry (1980) reported concerns by aircraft flight crews that a loss of proficiency will occur with extensive use of automatic equipment. Wiener (1988) reported that in response to these concerns pilots were routinely operating in manual mode in order to maintain flight skills. Furthermore, Wiener (1985) recommended as a result of his field studies that crews be given ‘turn-it-off training’. Similarly, Moray (1986) suggests the need to train operators with the appropriate models to operate systems manually, so that if automation fails, operator will be able to perform and take over control. This assumes, however, that the operators will detect the failure in the first place.

Indeed, there is evidence that manual skills are important for detecting the need for manual performance. Kessel and Wickens (1982) investigated the detection of system failures, which in their study were changes in dynamics associated with an automated tracking task. They found that although detection of changes in system dynamics was always better in manual mode, prior experience with operating in manual mode led to superior performance in

the automated mode when compared with performance of subjects who had operated only in automated mode. They attributed their finding to the development of internal models when operating in manual modes. These models directed attention to important cues relevant in automated mode. They also found that subjects performed significantly worse when they switched to manual mode and concluded that the internal models developed in automated mode did not transfer to performance in manual mode. Parasuraman (1992) (cited in Endsley and Kiris, 1995) also found improvements in system failure detection by having operators assume manual control at periodic intervals.

Endsley and Kiris (1995) found subjects were slower in manual task performance following the breakdown of the automated system under full automation than under partial automation. These conclusions support the importance of manual experience in developing skills relevant to the detection of automation failures.

Manual skills are required as long as people are required to intervene in the case of a disturbance. Experience of manual operation even helps in detecting system anomalies. High levels of automation provide very little opportunity to practise manual skills, which may result in the degradation of manual skills and an even greater reliance on automation. Training in manual operation of systems, as well as periodic 'turn-it-off training' can help to maintain skills.

2.6.3.3 Time

One of the explicit goals of ATC automation is to reduce separation minima in order to increase capacity. Hence, the time available to respond safely to an emergency scenario will be diminished (by decreased separation), just as the time required (recovery response times) may well be increased by out-of-the-loop unfamiliarity. Other factors decreasing time available will include traffic load (likely due to traffic growth) and traffic complexity (likely due to traffic growth, possible due to free flight). Based on research findings in the literature, Wickens (1999) proposed a hypothetical model of this trade-off. At high levels of automation more time is required to respond, while less time is available to recover due to complacency, lower SA and reduced manual skill. At low levels of automation less time is required to respond, while more time is available to recover.

2.6.3.4 Errors

'Human error reduction' was once seen as a natural consequence of automation; system designers thought that if human operators could be moved to the fringes, the risk of human error would decrease. But this premise was questioned (Wiener and Curry, 1980) and the real situation is still being revealed. On the basis of experimental studies and operational experience, many commentators asserted that automation produces new error forms or additional sources of errors (Wiener, 1988; Sarter and Woods, 1995). Another

view is that 'computers do not produce new sorts of errors. They merely provide new and easier opportunities for making the old errors' (e.g. Kletz, 1988). It is also a widely held view that the consequences of errors that do occur are likely to be more serious (Weiner, 1985; Billings, 1988; Leroux, 2000).

Experience has shown that automation does not eliminate human error. While automation may reduce or eliminate some errors, people will make errors in their new functions and produce new error forms, such as incorrect inputs into devices, mode confusion and error as a result of being unaware of system status. Two high-level classes of error can be identified:

- *omissions*, which are failures to respond to system irregularities;
- *commission* errors, where the human incorrectly follows an automated directive or recommendation without verifying it against other available information or in spite of contra-indications from other sources of information, known as an 'automation bias' (Mosier *et al*., 1994; 1997; Skitka *et al*., 1996).

It is hypothesised that such errors may result from the use of automation as a heuristic replacement for vigilant information seeking and processing in decision-making. Mosier and Skitka (1998) found that training on the 'automation bias' phenomenon had no significant effect on experienced pilots but had an effect of reducing commission errors in student participants. Their finding implied that early instruction on automation bias (i.e. before individuals have much experience with highly reliable automated systems) may be effective in instilling the practice of seeking information confirming automated recommendations before taking action.

Automation does not eliminate human error. Instead, errors take on new forms, often related to the detection, interpretation/diagnosis, or mitigation/correction of a problem.

2.6.3.5 Feedback

Endsley and Kiris (1995) found that SA and decision time was negatively affected following system breakdown. In addition, serious errors may occur when the automation fails if the system does not provide the operator with the needed information to update SA and detect failure occurrence and take over manual control. However, they found that ability to recover from automation failure was better, out of loop performance decrements decreased and SA increased when subjects used intermediate levels of automation as compared to full automation.

2.6.3.6 Equipment restoration

The issue of 'correction' or equipment restoration raises two significant questions regarding the application of automation (Wickens *et al*., 1997): 'Will [system control] specialists be able to effectively restore equipment and systems to service when (1) the equipment or systems that have failed contain automation on which air traffic controllers rely heavily to perform their duties and when (2) [system control] itself relies on automation to perform the restoration, but the automation has failed or is difficult to work with?' (p. 185). Wickens *et al*. call this a 'double indemnity situation'.

Wickens *et al*. (1997) report that one option frequently considered by system control personnel during system disturbances is to do nothing, since some of these disturbances are transient and such systems sometimes self-correct. Self-stabilisation is an important feature of automation.

2.6.3.7 Interview findings

Again, at this stage of recovery the ATC and system control activities will differ. Ultimately ATC will be concerned with ensuring aircraft are safely separated (mitigation), while system control will be concerned with restoring the system (correction). For ATC, a steady state (i.e. not deteriorating any further) should be attained, which is safe as far as traffic under control is concerned. In other words, mitigation may not permit controllers to continue to provide the same service that would have been possible if all radar had been available. However, it would at least allow controllers to recover the situation well enough so that existing flights continue safely (although any further aircraft entering the airspace may be restricted).

Methods involved in mitigation may involve the following:

- imposition of flow restrictions,
- utilisation of emergency separation,
- reversion to a 'manual mode',
- degraded operation,
- continue in fallback mode or use backup equipment,
- use or share other equipment (e.g. radar display),
- staffing recall and changes to staffing arrangements.

These are not separate strategies but rather aspects of ATC mitigation that may often be seen together.

Flow restrictions to limit the amount of air traffic entering a section of airspace will be necessary for many major disturbances, particularly problems that affect multiple sectors. Such interventions, though disruptive, are very effective at maintaining a safe (although restricted) service. For example, in the event of loss of all radar services, the primary ATC mitigation strategy is to restrict the flow of further aircraft, as well as expediting the transfer of existing traffic to adjacent units. This obviously requires immediate liaison with adjacent units.

In one centre, in case of problems with the FDP system, adjacent units are notified and flow managers apply a zero flow rate to all external sectors – effectively stopping new traffic entering the centre's airspace. At the appropriate time, sector flow rates are then carefully increased under this regime to a safe, manageable level. Departures from airfields are also gradually increased from zero up to a manageable rate. At all times, watch management scrutinise the operation to ensure that controllers do not become overloaded.

Emergency separation may have to be applied in some circumstances to provide more flight levels. It was stated that controllers would have to provide horizontal separation and emergency vertical separation (500ft). One controller stated that recovery from total loss of radar cover would be poor. Many controllers at one centre had not been trained in how to use primary radar only in the event of a loss of SSR.

In some cases, staff must be recalled to help deal with the recovery process. In one centre, in the case of a FDP failure or loss of System Flight Server (SFS), all staff are recalled to the control room to help handle traffic that is already in the airspace. Controllers may work as 'man and boy' (one controller will take executive control, while the other will write on flight progress strips and coordinate traffic), with the aim to achieve stable manual operation as quickly as possible.

Mitigation may involve reversion to a 'manual mode'. In case of problems with FDP, if no recovery has occurred six minutes after the initial indication, one centre visited declares 'manual operations' – i.e. loss of all electronics such as electronic coordination by Planner controllers. Manual coordination is also required in the case of other failures, such as the loss of SFS.

Similarly, controllers at one centre reported receiving strips late (after the aircraft has entered the sector) due to software problems. In such cases, an assistant my have to manually input aircraft details, or else write on blank strips.

Certain failures result in operation in a degraded mode. In the event of loss of Multi-radar Processing (MRP), controllers in one centre select a single source of radar data appropriate to their airspace to restore their radar picture. To provide controllers with an instant fallback (whilst they act to restore their own radar picture), the sector assistant's display is always derived from a single radar source. The coverage from a single source of data may not be as good as coverage from multiple sources. Furthermore, with reversion to a single radar source, new aircraft entering the sector are not shown as 'foreground tracks', the exit flight level will no longer be shown on track data blocks and (importantly) STCA will not function, until multi-radar services are restored. At another centre, if it is a large radar site, ATC separation is increased because radar tracking may be less accurate. This example shows both degraded operation and the use of backup equipment. Procedural control could be seen as another form of degraded mode, as would be required if radar were not available.

There are many other examples of the use of backup equipment or a fallback mode. In the situation of loss of all radar services, controllers in one centre ensure procedural separation exists by use of the electronic and paper flight progress strips. Controllers in the same centre stated that, in the event of loss of Voice Control System (VCS), they would make use of a backup radio telephone system. This provides limited two-way communications on a number of frequencies, using a dedicated handset at the workstation connected via telephone lines to discrete transmitters around the country. When system control notifies ATC that the VCS is functioning again, controllers at each workstation reselect the appropriate sector frequencies on their VCS panel. In another centre backup frequencies and mobile telephones are available. However, it was stated that backup equipment itself may not be functioning properly. The proper functioning and maintenance of backup equipment are clearly crucial to recovery.

In other cases equipment may be shared. In the case of a workstation failure ATCOs in the centres visited could share the adjacent controller's display (or use a fallback mode). The (redundant) design of such systems ensures that even major failures would normally only affect every other display. Otherwise, controllers on a sector may need to move to a standby suite and re-open their respective positions there, for instance if a telephone failed for a substantial period of time.

Reversion *back* to automatic mode can present many challenges. In the case of loss of a national FDP system, loss of link to the system or loss of a FDP-related server at one centre controllers have to switch from manual operations (with handwritten spare flight progress strips) back to electronic operation (where paper strips will be automatically produced). This implies high workload. To safely facilitate reversion to an electronic operation, it may be necessary to reduce the traffic levels to below the stable levels that may have been achieved. Traffic flow regulation with a zero rate may have to be re-applied until the traffic reduces to the point where reversion is possible. Although the link to the FDP system may be available again, full recovery may not be possible until late at night, when the traffic levels are very low. With full recovery, adjacent units are notified and sector flow rates are re-established, whilst operational stability of the FDP system and link is monitored. Electronic coordination restarts and handwritten strips are no longer necessary.

Synchronisation is also necessary during reversion back to automatic mode. In the event of VCS failure, to avoid the possibility of interference between mains transmitters and backup receivers, the recovery from backup to normal VCS operation is synchronised across the control room.

The other aspect of recovery is correction of the failure. This is normally, but not always, a system control or engineering task. Again, this may be done in several ways. Where the failure is software-related, correction may involve recovering software, often to a previous version, or entering new system parameters. Hardware failures will involve replacing a component. Interviewees at one centre reported a problem with graphics cards (bad oscillation), causing data corruption. In this case every card had to be

changed and engineers checked the radar picture every week. During these periods controllers switched to the fallback mode.

In other cases a subsystem may need to be restarted or a system may have to be 'refreshed' as quickly as possible. For instance, in one centre, when the problem causing the loss of FDP information has been rectified and full electronic functioning has been recovered, the entire system has to be 'refreshed' with new FDP data.

In some cases 'correction' is achieved by the controller rather than the engineer. For instance, in the case of code-callsign and squawk problems controllers in two centres reported that they could take control of a track using system functions and correct the erroneous data.

Not surprisingly, recovering from previously unknown and therefore unanticipated system failures can be extremely difficult to cope with, both for controllers and system control personnel. In these situations there may be no prescribed or appropriate recovery activities. For novel system problems the use of existing recovery strategies may at best provide limited assistance and at worst may be ineffective or even counter-productive. It is likely that in such situations, severe restrictions will be put on traffic until the problem is properly diagnosed and effectively overcome. Following an unanticipated failure, there are usually mechanisms in place to learn lessons, establishing necessary preventative measures and recovery procedures.

At this stage of recovery ATC will be concerned with ensuring that aircraft be safely separated (mitigation), while system control will be concerned with restoring the system (correction). Mitigation can take several forms, such as flow restrictions, emergency separation, manual modes of operation, degraded operation, fallback modes, shared equipment and staffing recalls. Correction of the technical failure may involve software recovery, system restarts or component replacement.

2.6.3.8 Communication and teamwork

Managing system disturbances is clearly not an individual process. The discussion above illustrates the involvement of both ATC and engineering personnel. Given the importance of team activities to system performance, this should be taken into consideration in evaluating the management of system disturbances. To date, research on team interaction in the ATM operational control under conditions of system disturbance is very rare.

Case studies, for example the USS Vincennes incident or the Staines Trident disaster, illustrate that stress can be induced by uncertainty, ambiguity and time pressure, reducing a team's flexibility and causing errors. Under high stress, team members thought processes may be disrupted (Janis and Mann, 1977). However, an increase in the level of stress does not necessarily result

in a decrease in the team's outcome performance (Serfaty, Entin and Volpe, 1993). The primary adaptation mechanism that allows teams to maintain and improve their performance under a high level of time pressure may be a switch from explicit to implicit coordination[6] (Entin and Serfaty, 1999). Implicit coordination involves the use of shared or mutual mental models among team members (Cannon-Bowers and Salas, 1990). It involves two components: 1) a common or consistent model of the actual situation and 2) a set of mutual mental models about other team-member functions. These allow team members to *pre-empt* the actions and needs of another so that actions can be coordinated and needs met without explicit communication.

Effective shared mental models can be developed during periods of low workload and implemented during periods of high workload (Orasanu, 1990). Team performance can also be improved via training in strategies aimed at developing mutual mental models of each team member's tasks and abilities, improving anticipatory behaviour of team members and managing coordination and communication overheads. Hence, high performing teams adapt to stressful situations by adapting not only their decision-making strategy but also their coordination and communication strategy, as well as behaviour to the demands of the situation to maintain performance or minimise perceived stress.

A study of team interaction in ATM was conducted at the National Air Traffic Services (NATS) London Area and Terminal Control Centre (LATCC) (Randall and Harper, 1995). The study found that much of the individual work done by controllers is done in a way that makes available to other controllers information regarding the state and conduct of the task, without requiring overt messaging between controllers. It notes two aspects of the social organisation of ATM work that have consequences for automation and safety. The first aspect is that errors are handled and safe working is manifested via the collective attention to paper-based information. The second is that the culture of support and 'inter-suite' attentiveness is achieved via active coordination. Controllers support each other in various ways, including checking of data by all members of the team, mutual attentiveness and the drawing of attention to significant information changes.

Randall and Harper's (1995) study concluded that the social and team interaction was a semi-formalised feature of work at LATCC, a manifestation of controller culture, where cooperation, helpfulness, and endeavouring to explain one's purposes and reasoning are for mutual benefit. Development of new ATC systems that interfere with, restrict or block this interaction may reduce the socio-technical systems' effectiveness.

The observations of this study are consistent with components of implicit coordination mentioned before. However, the study does not suggest how culture of support can be assessed or what aspects of the interaction should be assessed in order to examine the team interactions which are relevant to

[6] The term 'coordination' in their literature (more akin to 'teamwork') is not to be confused with the term 'coordination' as it is used in ATM.

performance and more importantly associated with performance with automation and during automation failure.

Multitasking is a key characteristic of ATM. An understanding of how a group multi-tasks is important to understand how team interaction will be impacted by the introduction of automation. A model of work group multitasking behaviour is shown in Figure 2 (Waller, 1995). Research on coordination processes in groups suggests that resource allocation in groups is an important factor in overall group performance (Shiflett, 1973).

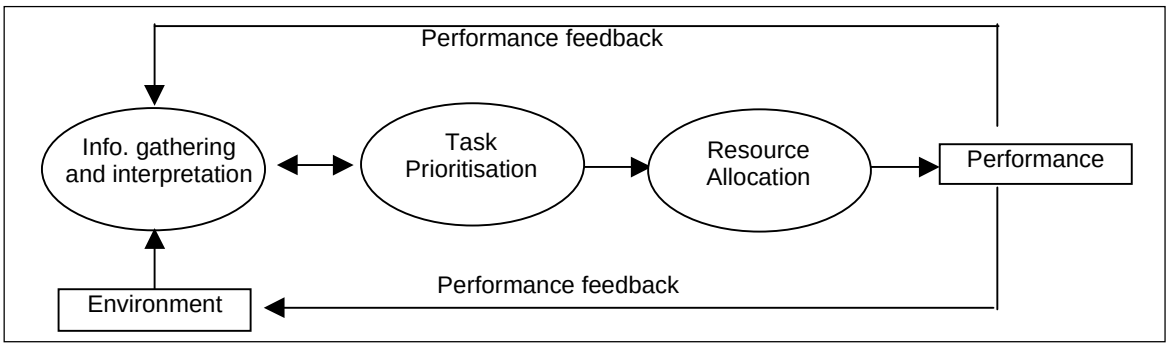


Figure 2: Model of work group multitasking behaviour (from Waller, 1995)

The first module of the model is information gathering and interpretation, which consists of information acquisition, information evaluation and integration of outcomes from these activities. Team members identify group tasks to achieve group goals. Members receive or collect information about group tasks or goals from the environment by: 1) proactively seeking out information from team members or the environment regarding tasks awaiting performance, the state of tasks being performed (e.g. whether a task has been performed to the satisfaction of others outside the group) or organisational factors; 2) passively or reactively receiving information from other team members or the environment regarding task performance.

The second module in the model is task prioritisation, which proposes that team members develop a shared understanding of relative task importance. The task prioritisation module compares tasks awaiting performance to other tasks on a number of different dimensions such as familiarity, relative difficulty, the source, and the relative status, power or immediacy attached to the task by that source. It also takes into account the status of the task in terms of any interdependence among tasks being prioritised.

The third module, resource allocation, concerns the application of group resources to prioritised tasks awaiting performance. Team members adopt different strategies for task performance depending on the characteristics of a particular task combination. These strategies are group level time-sharing and time-swapping. Team effectiveness depends heavily on effective resource management; the team shares information effectively and is appropriately coordinated in their monitoring and task performance responsibilities (Huey and Wickens, 1993).

Managing system disturbances requires teamwork, within and between the ATC and engineering staff. Stressful situations can make teamwork more difficult, but performance can be maintained if team members can communicate more implicitly, a skill enabled by shared mental models. Work-group multitasking is also crucial to recovery success. This involves information gathering and interpretation, task prioritisation and resource allocation.

2.6.3.9 Interview findings[7]

Communication between team members becomes even more important in abnormal operations such as those found during system disturbances. Communication takes place between several parties. For instance, on detecting a disturbance, a controller may communicate with another controller to check whether a disturbance is being experienced by just him or her, by the whole sector, by whole control room, etc. The controller may then communicate with the watch supervisor, to report the problem. The watch supervisor might then communicate with system control to report the problem. Alternatively, a controller might communicate directly with system control. If system control detects a disturbance, engineers will normally communicate with the watch supervisor, who will relay the message to those affected.

In dealing with the problem (mitigation) controllers will again need to communicate with other controllers, for instance to transfer aircraft to other units. Supervisor may need to communicate with other supervisors, with flow control, etc. Similarly, system control personnel will need to communicate with each other to diagnose and correct the problem, and may need to communicate with remote engineers in other units and sites.

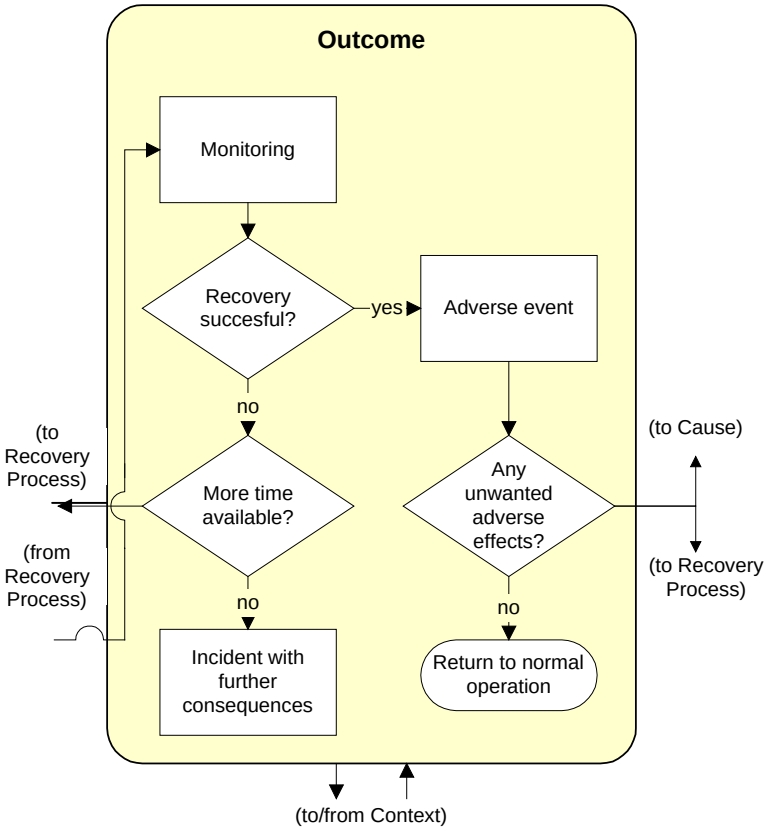
System control will also need to communicate with the watch supervisor to inform him or her about cause (though not in all cases), manifestation, extent and likely duration of the problem, the progress of the resolution, and will again need to communicate once the problem has been finally corrected. The watch manager will decide whether to disseminate this information to controllers.

Communication between ATC and system control can be a problem due to different backgrounds and knowledge, which introduce a language barrier. Hence, communication can take longer than it would if this disparity did not exist and errors can, of course, be introduced.

[7] See also Section 2.2.7.

The chain of communication during disturbances can involve a variety of personnel. This should be planned for different types of failures and optimised, so that the most efficient and effective arrangement is reached. Personnel from ATC and engineering backgrounds should also be trained together to increase understanding of each other's needs.

2.7 Outcome



2.7.1 Monitoring

Although the main recovery process is characterised by detection, interpretation or diagnosis and mitigation or correction, these activities by no means conclude the process. Prior to this stage, personnel have made an attempt to resolve the problem and its implications; they do not know whether the attempt has been successful. Hence, once corrective activities have been performed, there will be a period of post-mitigation monitoring by ATC personnel and post-correction monitoring by engineering personnel to assessment of the outcome of the correction (Shorrock and Scaife, 2001). This involves ensuring that an acceptable (e.g. steady) system state has been reached, or that the failure itself has been resolved, and the air navigation service is back to normal. Research on performance at this stage is rare. It would appear that at this stage the human performance requirements would be similar to performance requirements at the detection stage. However, a key difference is that during monitoring, controllers and engineers will be driven more by 'top-down' processes, primarily expectation. Since these personnel will have knowledge of the failure and disturbance, and its cause, they will also likely have expectations – either specific or general – about how the system might behave following correction and mitigation. For instance, personnel may expect other related problems (common-mode or common-cause failures), or expect that the same problem may recur. Otherwise, personnel may have a general expectation or suspicion that something else may go wrong, because the system is in an unstable state.

On the basis of a period of monitoring, for a time deemed appropriate by the individual (unless such a time is laid down by procedures), or following a number of active checks, the controller and the engineer must decide whether recovery (or more specifically, mitigation and correction) has been successful. The controller will be interested primarily in the safety of air traffic and the engineer will be interested primarily in the behaviour of the technical system.

Recovery will be regarded as either successful or unsuccessful. It may be successful for the engineer but not for the controller, or vice versa.

2.7.2 Successful recovery

If initial recovery is judged successful, then an ‘adverse event’ has occurred. However, the recovery actions may have other adverse effects (an operational or technical complication) either in the shorter- on longer-term. Operational complications (side-effects of controller mitigation) signal a return to the mitigation stage of the recovery process, while technical complications (side effects of engineer correction activities) will mean a return to the ‘cause’ stage of the RAFT Framework.

2.7.3 Unsuccessful recovery

If recovery is not successful, the RAFT Framework supposes that, if more time is available, the controller or engineer (or both) will return to either diagnosis (to determine the real cause of the problem) or correction and mitigation (to retry the strategy or attempt a new strategy without deeper interpretation or diagnosis). If further monitoring proves that these further actions are not successful, then the cycle of renewed efforts at recovery can be repeated. However, if no time is available, the result is an incident with further consequences.

2.7.4 Interview findings

Interviewees from the three centres indicted that monitoring is the role of system control, to verify that a function is available, or that data is reliable. However, naturally, controllers will monitor the function also, since trust will often be reduced. If recovery is successful, it is important that the engineer’s actions have not caused a further problem or complication. An engineer in one centre stated that it is also important that fixes developed in response to faults that appear to eliminate the problem, do not in fact mask the underlying problem. This could result in further unexpected system problems (for which there may be no recovery procedure in place).

Controllers may file an observation report where disturbances have occurred. However, a controller at one centre stated that the feedback loop is not properly closed and controllers are not informed of the outcome of a report; many files are closed with the comment ‘problem not found’. Controllers stated that loss of separation incidents had not occurred due to system failure. This is a significant finding, but does not guarantee or assure that this could not occur in the future.

Following mitigation and correction activities, a period of monitoring is necessary. The controller will be interested primarily in the safety of air traffic, and the engineer will be interested primarily in the behaviour of the technical system. On the basis of this, recovery will be regarded as either successful or unsuccessful. Complications may occur following successful recovery, or else recovery may be unsuccessful, requiring a return to earlier stages of the recovery process. Once problems are resolved it is important that everyone affected is informed of the reason for the fault and any future implication.

Page intentionally left blank

3. CONCLUSIONS

This report has discussed the human role in managing system disturbances, utilising research findings from both ATM and non-ATM domains, as well as findings from interviews with thirty ATM personnel in three European ATC centres. These findings are structured around a contextual framework, which itself is the basis for a tool for analysing how humans are likely to recovery from functional disturbances, called the **Recovery from Automation Failure Tool** (**RAFT**).

The interviews revealed many interesting findings regarding the management of system disturbances. In particular, the following key findings should be noted:

- many current technical failures do not result in a functional disturbance, primarily due to in-built system redundancy/duplication;
- future disturbances are likely to take on a more subtle form, related to data quality and integrity rather than functional availability;
- good procedures are not available in all centres to help controllers to deal with disturbances;
- many controllers did not have appropriate continuation training in recovery strategies;
- the communication and teamwork processes between all personnel involved in managing disturbances (particularly within and between ATC and engineering personnel) should be optimised;
- good practice in the area of the management of system disturbances is not shared among European Civil Aviation Conference (ECAC) States.

The RAFT Framework considers the context and cause of potential problems, the problem itself, the effect and exposure, the recovery process and the outcome. This report details research and operational experience regarding the management of system disturbances. RAFT itself provides a method for analysing functional disturbances and helps to consider systematically the concepts within the RAFT Framework. RAFT is available separately in electronic form. It is proposed that RAFT provides an appropriate predictive method for examining system disturbances in ATM, which can be verified using measures of recovery performance in simulated or operational environments. Further work is recommended to apply, test and refine the approach. Finally, it is suggested that a set of companion principles for human-automation integration be developed to help system designers to design automation systems with recovery ‘built-in’.

Page intentionally left blank

REFERENCES

Bainbridge, L. (1983). Ironies of automation. *Automatica*, 19, 775-779.

Bergeron, H.P. (1981). Single pilot IFR autopilot complexity/benefit trade-off study. *Journal of Aircraft*, 18, 705-706.

Billings, C.E. (1988). Toward human-centered automation. In: S.D. Norman and H.W. Orlady (Eds.), *Flight Deck Automation: Promises and Realities*. Moffett field, CA: NASA Ames Research Center, pp. 167-190.

Billings, C.E. (1991). Toward a human-centred aircraft automation philosophy. *International Journal of Aviation Psychology*, 1 (4), 261-270.

Bisseret, A. (1981). Application of signal detection theory to decision-making in supervisory control. *Ergonomics*, 24, 81-94.

Brehmer, B. (1987). Development of mental models for decision in technological systems. In: J. Rasmussen, K. Duncan and J. Leplat (Eds.), *New Technology and Human Error*, pp. 111-120, New York: John Wiley & Sons.

Cannon-Bowers, J.A. and Salas, E. (1990). Cognitive psychology and team training: Shared mental models in complex systems. Paper presented at the *5th Annual Conference of the Society for Industrial and Organisational Psychology*, Miami, FL.

Carmody, M.A. and Gluckman, J.P. (1993). Task specific effects of automation and automation failure on performance, workload and situational awareness. In: R.S. Jensen and D. Neumeister (Eds.), *Proceedings of the 7th International Symposium on Aviation Psychology,* Ohio State University, Columbus, OH, pp. 167-171.

Conejo, R. and Wickens, C.D. (1997). *The Effects of Highlighting Validity and Feature Type on Air-To Ground Target Acquisition Performance*. University of Illinois Institute of Aviation Technical Report (ARL-97-11/NAWC-ONR-97-1). Savoy, IL: Aviation Res. Lab.

Cowan, N. (1988). Evolving conceptions of memory storage, selective attention and their mutual contraints within the human information processing system. *Psychological Bulletin*, 104 (2), 163-191.

Craig, A. (1985). Vigilance: Theories and laboratory studies. In: S. Folkard and T.H. Monk (Eds.), *Hours of Work*, Chichester, UK: Wiley, pp. 107-121.

Davies, D.R. and Parasuraman, R. (1982). *The Psychology of Vigilance*. London: Academic Press.

EATMP (2000). *Human Resources Programme – Stage 1: Programme Management Plan*. Ed. 1.0. Brussels: EUROCONTROL.

EATMP Human Resources Team (2002). *Technical Review of Human Performance Models and Taxonomies of Human Error in ATM (HERA)*. HRS/HSP-002-REP-01. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2003a). *Guidelines for Trust in Future ATM Systems: A Literature Review*. HRS/HSP-005-GUI-01. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2003b). *Guidelines for Trust in Future ATM Systems: Measures*. HRS/HSP-005-GUI-02. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2003c). *Guidelines for Trust in Future ATM Systems: Principles*. HRS/HSP-005-GUI-03. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2003d). *The Development of Situation Awareness Measures in ATM Systems*. HRS/HSP-005-REP-01. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2003e). *Age, Experience and Automation in European Air Traffic Control*. HRS/HSP-005-REP-02. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATMP Human Resources Team (2003f). *The Human Error in ATM Technique (HERA-JANUS)*. HRS/HSP-002-REP-03. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2004a). *A Measure to Assess the Impact of Automation on Teamwork*. HRS/HSP-005-REP-07. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2004b). *Impact of Automation on Future Controller Skill Requirements and a Framework for their Prediction*. HRS/HSP-005-REP-04. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2004c). *A Tool for the Assessment of the Impact of Change in Automated ATM Systems on Mental Workload*. HRS/HSP-005-REP-03. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM Human Resources Team (2004d). *Age, Experience and Automation in European Air Traffic Control - Survey in the ECAC Area*. HRS/HSP-005-REP-05. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

EATM (2004e). *Air Navigation System Safety Assessment Methodology* SAF.ET1.ST03.1000-MAN-01*.* Edition 2.0. Released Issue. Brussels: EUROCONTROL*.*

Endsley, M.R. (1987). The application of human factors to the development of expert systems for advanced cockpits. *Proceedings of the Human Factors and Ergonomics Society 31st Annual Meeting*, pp. 1388-1392. Santa Monica, CA: The Human Factors and Ergonomics Society.

Endsley, M.R. (1993). Situation awareness and workload: flip sides of the same coin. In: R.S. Jensen and D. Neumeister (Eds.), Proceedings of the *Seventh International Symposium on Aviation Psychology*, pp. 906-911, Department of Aviation, The Ohio State University, Columbus, OH.

Endsley, M.R. and Kaber, D.B. (1999). Level of automation effects on performance, situation awareness and workload in a dynamic control task, *Ergonomics*, 42, 462-492.

Endsley, M.R. and Kiris, E.O. (1995). The Out-of-the-loop Performance Problem and Level of Control in Automation, *Human Factors*, 37, 381-394.

Endsley, M.R. and Smolensky, M.W. (1998). Situation awareness in air traffic control: the picture. In: M.W. Smolensky and E.S. Stein (Eds.), *Human Factors in Air Traffic Control*. London: Academic Press.

Entin, E.E. and Serfaty, D. (1999). Adaptive Team Coordination. *Human Factors*, 41 (2)*,* 312-325.

Garland, D. and Hopkin, V.D. (1994). Controlling automation in future air traffic control: The impact on situational awareness. In: R.D. Gilson, D.J. Garland and J.M. Koonce (Eds.), *Situational Awareness in Complex Systems.* Daytona Beach, FL: Embry-Riddle Aeronautical University Press.

Harwood, K., Sanford, B.D. and Lee, K.K. (1998). Developing ATC Automation in the Field: It Pays to Get Your Hands Dirty. *Air Traffic Control Quarterly*, 6 (10), 45-70.

Health and Safety Executive (2000). *Better Alarm Handling*. HSE Information Sheet - Chemicals Sheet No. 6., March.

Hopkin, V.D. (1995). *Human Factors in Air Traffic Control.* London: Taylor and Francis.

Hopkin, V.D. (1998). The impact of automation on air traffic control specialists. In: M.W. Smolensky and E.S. Stein (Eds.), *Human Factors in Air Traffic Control*, pp. 391-419. San Diego, CA: Academic Press.

Huey, B. and Wickens, C.D. (1993). *Workload Transition: Implications for Individual and Team Performance.* Washington, D.C.: National Academy Press.

Janis, I.L. and Mann, L. (1977). *Decision-making.* New York: Free Press.

Kanse, L. and van der Schaaf, T. (2000). Recovery from failures - understanding the positive role of human operators during incidents. In: D. de Waard, C. Weikert, J. Hoonhout and J. Ramaekers (Eds.), *Human-System Interaction: Education, Research and Application in the 21st Century*. Maastricht, Netherlands: Shaker Publishing.

Kessel, C. and Wickens, C.D. (1982). The transfer of failure detection skills between monitoring and controlling dynamic systems, *Human Factors,* 24, 49-60.

Kletz, T. (Ed.) (1988). *What Went Wrong? Case Histories from Process Plant disasters*. Houston: Gulf Publishing Company.

Kontogiannis, T. (1999). User strategies in recovering from errors in man-machine systems. *Safety Science*, 32, 49-68.

Lee, J.D. and Moray, N. (1992). Trust, control strategies and allocation of function in human-machine systems. *Ergonomics*, 35, 1243-1270.

Lees, F.P. (1980) *Loss Prevention in the Process Industries*, Vol. 1 & 2. London: Butterworths.

Leroux, M. (2000). Cognitive aspects and automation. In: N.B. Sarter and R. Amalberti (Eds.), *Cognitive Engineering in the Aviation Domain*. Mahwah, Hillsdale, NJ: Lawrence Erlbaum Associates, Inc. pp. 99-130.

Leveson, N.G. (1995). *Safeware: System Safety and Computers*. Addison-Wesley Publishing Company.

Low, I. and Donohoe, L. (2001). Methods for assessing ATC controllers' recovery from automation failure. In: D. Harris (Ed.), *Engineering Failure and Cognitive Ergonomics*, Vol. 5. Aldershot, UK: Ashgate Publishing.

Mackworth, N.H. (1957). Some factors affecting vigilance. *Advancements in Science*, 53, 389-393.

MacMillan, J., Deutsch, S.E. and Young, M.J. (1997). A comparison of alternatives for automated decision support in a multi-task environment. In: *Proceedings of the Human Factors and Ergonomics Society 41st Annual Meeting*, pp. 190-194. Santa Monica, CA: The Human Factors and Ergonomics Society.

Moray, N. (1986). Monitoring behaviour and supervisory control. In: K.R. Boff, L. Kaufmann and J.P. Thomas (Eds.), *Handbook of Perception and Human Performance*. Vol. II. New York: Wiley.

Mosier, K.L. and Skitka, L.J. (1998). Automation bias and errors: Are teams better than individuals. In: *Proceedings of the Human Factors and Ergonomics Society 42nd Annual Meeting*, pp. 201-205. Santa Monica, CA: The Human Factors and Ergonomics Society.

Mosier, K.L., Skitka, L.J., Heers, S. and Burdick, M.D. (1997). Patterns in the use of cockpit automation. In: M. Mouloua and J. Koonce (Eds.) *Human-Automation Interaction: Research and Practice,* pp. 167-173, Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Mosier, K.L., Skitka, L.J., Heers, S. and Burdick, M.D. (1998). Automation bias: Decision-making and performance in high-tech cockpits. *International Journal of Aviation Psychology*, 8(1), 47-63.

Mosier, K.L., Skitka, L.J. and Korte, K.J. (1994). Cognitive and social psychological issues in flight crew/automation interaction. In: M. Mouloua and R. Parasuraman (Eds.), *Human Performance in Automated Systems: Current research and trends*, pp. 191-197. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

NATS (2000). *Memorandum by National Air Traffic Services Ltd (NATS 02) to the Select Committee on Environment, Transport and Regional Affairs*, 29 September 2000. http://www.publications.parliament.uk.

Norman, D. (1990). The problem with automation: Inappropriate feedback and interaction, not over-automation. In: *Proceedings of the Royal Society of London*, B237, 585-593.

Nuechterlein K.R., Parasuraman, R. and Jiang, Q. (1983). Visual sustained attention: Image degradation produces rapid sensitivity decrement over time. *Science*, 220, 327-329.

Orasanu, J.M. (1990). *Shared Mental Models and Crew Decision-making* (CSL Report No. 46). Princeton University, Cognitive Science Laboratory.

Parasuraman, R. (1987) Human-computer monitoring. *Human Factors*, 29, 695-706.

Parasuraman, R. (1993) Effects of adaptive function allocation on human performance, In: D.J. Garland and J.A. Wise (Eds.), *Human Factors and Advanced Aviation Technologies*, Daytona Beach, FL. Embry-Riddle Aeronautical University Press, pp. 147-158.

Parasuraman, R., Molloy, R. and Singh, I.L. (1993). Performance consequences of automation induced complacency, *International Journal of Aviation Psychology*, 3, 1-23.

Parasuraman, R., Molloy, R. and Singh, I.L. (1994). Monitoring automation failures in human-machine systems. In: M. Mouloua and R. Parasuraman (Eds.), *Automation and human performance: Recent research and trends,* pp. 8-14. Hillsdale, NJ: Erlbaum Lawrence Associates, Inc.

Parasuraman, R. and Riley, V. (1997). Humans and Automation: use, misuse, disuse, abuse. *Human Factors*, 39 (2), 230-253.

Parasuraman, R., Sheridan, T.B. and Wickens, C.D. (2000). A model for the types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans*, 30, 286-297.

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Randall, D. and Harper, R. (1995). Cooperative work and technological support in Air Traffic Control. In: N. McDonald, N. Johnston and R. Fuller (Eds.), *Applications of psychology to the aviation system*, Vol. 1, pp. 223-228. Aldershot, UK: Ashgate Publishing.

Roske-Hofstrand, R.J. and Murphy, E.D. (1998). Human information processing in air traffic control. In: M.W. Smolensky and E.S. Stein (Eds.), *Human Factors in Air Traffic Control*. London: Academic Press.

Rouse, W.B. and Morris, N.M. (1985). *On looking into the black box: Prospects and limits in the search for mental models*. DTIC No. AD-A159080. Center for Man-Machine Systems Research, Georgia Institute of Technology, Atlanta, GA.

Sarter, N. and Woods, D.D. (1995). How in the world did we ever get into that mode? Mode error and awareness in supervisory control. *Human Factors*, 37 (1), 5-19.

Satchell, P. (1993). *Cockpit monitoring and alerting systems.* Aldershot, U.K.: Ashgate Publishing.

Sawin, D.A. and Scerbo, M.W. (1994). Vigilance: How To Do It and Who Should Do It. In: *Proceedings of the Human Factors and Ergonomics Society 38th Annual Meeting "People and Technology in Harmony"*, Nashville, Tennessee, October 24-28, 1994, Vol. 2, pp. 1312-1316. Santa Monica, CA: The Human Factors and Ergonomics Society.

Serfaty, D., Entin, E.E. and Volpe, C. (1993). Adaptation to stress in team decision-making and coordination. In: *Proceedings of the Human Factors and Ergonomics Society 37th Annual Meeting*, pp. 1228-1232. Santa Monica, CA: The Human Factors and Ergonomics Society.

Sheridan, T. (1980). Computer control and human alienation, *Technology Review*, 10, 61-73.

Shiflett, S.C. (1973). Performance effectiveness and efficiency under different dyadic work strategies. *Journal of Applied Psychology*, 57, 257-263.

Shorrock, S.T. and Scaife, R. (2001). Evaluation of an alarm management system for an ATC centre. In: D. Harris (Ed.) *Engineering Psychology and Cognitive Ergonomics: Volume Five - Aerospace and Transportation Systems*. Aldershot, UK: Ashgate Publishing.

Shorrock, S.T., Scaife, R. and Cousins, A. (2002). Model-based principles for human-centred alarm systems from theory and practice. Proceedings of the *21st European Annual Conference on Human Decision-making and Control*, 15th and 16th July 2002, The Senate Room, University of Glasgow.

Singh, I.L., Molloy, R. and Parasuraman, R. (1993). Automation-induced "complacency": Development of the complacency-potential rating scale. *International Journal of Aviation Psychology*, 3, 111-121.

Singh, I.L, Molloy, R. and Parasuraman, R. (1997). Automation-induced monitoring inefficiency: role of display location. *International Journal of Human-Computer Studies*, 46, 17-30.

Skitka, L.J., Mosier, K.L. and Burdick, M. (1996). Accountability and automation bias. Paper presented at the Eighth Annual American Psychological Society Conference, San Francisco, CA.

Slamecka, N.J. and Graf, P. (1978). The generation effect: Delineation of a phenomenon. *Journal of Experimental Psychology: Human Learning and Memory*, 4, pp. 592-604.

Swann, C.D. (1999). Ergonomics of the design of process plant control rooms. In: IEE, People in Control: An International Conference on *Human Interfaces in Control Rooms, Cockpits and Command Centres*, Bath, 21-23 June 1999.

Taylor, R.M., Finnie, S. and Hoy, C. (1997). Cognitive rigidity: The effects of mission planning and automation on cognitive control in dynamic situations. In: *Proceedings of the 9th International Symposium on Aviation Psychology*, pp. 415-421. Columbus, OH: Dept of Aviation, The Ohio State University.

Teichner, W.H. (1974). The detection of a simple visual signal as a function of time on watch. *Human Factors*, 16, pp. 339-353.

Thackray, R.I. and Touchstone, R.M. (1989). Detection efficiency on an air traffic control monitoring task with and without computer aiding, *Aviation, Space and Environmental Medicine*, 60, pp. 744-748.

Vortac, O.U. (1993). Should Hal open the pod bay doors? An argument for modular automation. In: D.J. Garland and J.A. Wise (Eds.), *Human factors and advanced aviation technologies,* pp. 159-163. Daytona Beach, FL: Embry-Riddle Aeronautical University Press.

Waller, M.J. (1995). Work group multitasking in aviation. In: N. McDonald, N. Johnston and R. Fuller (Eds.), *Applications of Psychology to the Aviation System*, Vol. 1, pp. 256-261.

Warm, J.S., Dember, W.N. and Hancock, P.A. (1996). Vigilance and workload in automated systems. In: R. Parasuraman and M. Mouloua (Eds.), Automation and Human Performance: Theory and Applications, Hillsdale, NJ: Erlbaum.

Wempe, T. (1965). Effects of gust-induced and manoeuvring acceleration stress on pilot-vehicle performance. *Aerospace Medicine*, 36, 246-255.

Whitfield, D., Ball, R.B. and Ord, G. (1980). Some human factors aspects of computer-aiding concepts for air traffic controllers. *Human Factors*, 22, 569-580.

Wickens, C.D. (1992). *Engineering Psychology and Human Performance.* 2nd Edition. New York: Harper Collins.

Wickens, C.D. (1999). Automation in air traffic control: Human performance issues. In: M.W. Scerbo and M. Mouloua (Eds.), *Automation Technology and Human Performance: Current research and trends,* 2-10. Mahwah, New Jersey: Erlbaum Lawrence.

Wickens C.D, Mavor, A. and McGee, J.P. (Eds.) (1997). *Flight to the Future: Human Factors in Air Traffic Control.* Washington, DC: National Academy Press.

Wiener, E.L. (1981). Complacency: Is the term useful for air safety? Proceedings of the *26th Flight Safety Foundation Seminar on Human Factors in Corporate Aviation*, Denver, US, pp. 116-125.

Wiener, E.L. (1985). Beyond the sterile cockpit. *Human Factors*, 27, 75-90.

Wiener, E.L. (1988). Cockpit automation. In: E.L. Wiener and D.C. Nagel (Eds.), *Human Factors in Aviation*, pp. 433-461. San Diego, CA: Academic Press.

Wiener, E.L. and Curry, R.E. (1980). Flight deck automation: Promises and problems. *Ergonomics*, 23, 995-1011.

Woods, D.D. (1993). The price of flexibility in intelligent interfaces. *Knowledge-Based Systems*, 6, 1-8.

Woods, D.D. (1996). Decomposing automation: Apparent simplicity, real complexity. In: R. Parasuraman and M. Mouloua (Eds.), *Automation and Human Performance: Theory and Applications,* pp. 3-17. Hillsdale, NJ: Erlbaum Lawrence Associates, Inc.

Yeh, M., Wickens, C.D. and Seagull, J. (1998). *Effects of Frame of Reference and Viewing Condition on Attentional Issues with Helmet Mounted Displays*. University of Illinois Institute of Aviation Technical Report (ARL-98-1/ARMY-FEDLAB-98-1). Savoy, IL: Aviation Res. Lab.

FURTHER READING

EATMP Human Resources Team (2000). *Guidelines for Personal and Career Development Processes.* HUM.ET1.ST03.1000-GUI-01. Ed. 1.0. Released Issue. Brussels: EUROCONTROL.

Page intentionally left blank

ABBREVIATIONS AND ACRONYMS

For the purposes of this document the following abbreviations and acronyms shall apply:

ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATCO	Air Traffic Controller / Air Traffic Control Officer *(US/UK)*
ATICCC	Air Traffic Incident Coordination and Communication Cell
ATM	Air Traffic Management
BGS	Basic Global Services
CMS	Control Monitoring System
DAP	Director(ate) ATM Programmes *(EUROCONTROL Headquarters, SD)*
DAS	Director(ate) ATM Strategies *(EUROCONTROL Headquarters, SD)*
DAS/HUM *or just* HUM	Human Factors Management Business Division *(EUROCONTROL Headquarters, SD, DAS)*
EATCHIP	European Air Traffic Control Harmonisation and Integration Programme *(later renamed 'EATMP' and today known as 'EATM')*
EATM(P)	European Air Traffic Management (Programme) *(formerly known as 'EATCHIP')*
ECAC	European Civil Aviation Conference
EMT	Eye Movement Tracking
ET	Executive Task *(EATCHIP)*
FDP	Flight Data Processing
FFP	Flight Plan Processing
HF	Human Factors

HFFG	Human Factors Focus Group *(EATM, HRT)*
HRS	Human Resources Programme *(EATM(P))*
HRT	Human Resources Team *(EATM(P))*
HSP	Human Factors Sub-Programme *(EATM(P), HRS)*
IANS	Institute of Air Navigation Services (*EUROCONTROL Luxembourg)*
LAN	Local Area Network
LATCC	London Area and Terminal Control Centre
MRP	Multi-radar Processing
NAS	National Airspace System *(UK)*
NATS	National Air Traffic Services Ltd. *(UK)*
OSH	Operational System Hazard
RAFT	Recovery from Automation Failure Tool
REP	Report *(EATM(P))*
R/T	Radiotelephony
RTF	Radiotelephone / radiotelephony
SA	Situation Awareness
SAF	Safety
SAGAT	SA Global Assessment Technique
SAM	Safety Assessment Methodology *(EUROCONTROL)*
SD	Senior Director, EATM Service Business Unit *(EUROCONTROL Headquarters)*
SFS	System Flight Server
SHAPE (Project)	Solutions for Human-Automation Partnerships in European ATM (Project) *(EATM(P), HRS, HSP)*
SRP	Single Radar Processing
SSR	Secondary Surveillance Radar
ST	Specialist Task *(EATCHIP)*

STCA	Short-Term Conflict Alert
TAIC	Transport Accident Investigation Commission
VCS	Voice Control System
VDU	Visual Display Unit
VHF	Very High Frequency

Page intentionally left blank

CONTRIBUTORS

The contribution of the Members of the HRT Human Factors Sub-Group (HFSG), now known as the Human Factors Focus Group (HFFG), to this document during the group meetings, and further written comments, were much appreciated.

Special thanks are also given to the controllers and centres participating in the questionnaires and interviews on managing system disturbances.

Document configuration

C. HELLINCKX
(external contractor)
EUROCONTROL Headquarters

Page intentionally left blank

APPENDIX: INTERVIEW BRIEF

SHAPE Project – Managing System Disturbances: *Information Gathering*

The EUROCONTROL 'Solutions for Human Automation Partnership in European ATM (SHAPE)' Project is looking at the effects of automation on human performance and future ATM. Part of this study focuses on the ability to manage system disturbances that directly impact the air traffic controller. It is vital to the study to obtain a clear indication of how a variety of personnel (watch managers, controllers, ATM engineers, etc.) recover from problems in order to guide how future automation might impact on this.

Possible failures

We are focussing on failures of information display or control functions, e.g.:

- *Total loss of data availability* - Total loss of information or function (e.g. loss of radar services due to an unidentified single point of failure, workstation failure, coordination request sent by controller but not received by intended recipient).

- *Partial availability of data* - Partial loss of information or function (e.g. SSR code failure, interference on RTF).

- *Loss of redundancy* - No loss of information or function, but some loss of redundancy (e.g. operation in fallback mode using a single radar source).

- *Loss of data integrity* - Data appears credible but has low integrity (e.g. code-callsign database failure, Mode C height readout not accurate).

- *Data corruption* - Data available but obviously corrupted (e.g. unreadable text and/or graphics on the radar display).

- *Extra data* - More data than intended or expected (e.g. ghost tracks on the radar display).

- *Performance timing problem* - Information or function available but data processing is too slow or fast (e.g. slow update of workstation displays, late coordination requests).

Information gathering

To obtain pertinent information it is necessary to interview those directly involved in ATM operations (in various European centres) that have to deal with recovery from system failure. We are interested in the following issues:

- Are there any strategies or plans for system recovery activities?

- Is the recovery process based on a set procedure or is it *ad hoc*, or does it depend on the nature of the failure?

- What kinds of system failure or fault that may affect the ATCO occur currently or have occurred?

- How did you deal with them and what were the outcomes? (Detection of the problem? Diagnosis of the problem? Correction of the problem? Monitoring following correction? Outcomes?)

- What are the current challenges or difficulties in recovering from system failures?

- Are existing communication processes/facilities sufficient for effective recovery from system failures?

- Is there additional assistance available to help during recovery procedures and, if so, is the teamwork effective?

We are interested in failures that you have personally had to deal with and those that **could occur**. We plan to interview a number of individuals in different roles, each for around 30-45 minutes. Names of interviewees are not recorded. We are most grateful for your support.