EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

EUROCONTROL EXPERIMENTAL CENTRE

INDIVIDUAL AND GROUP APPROACHES TO HUMAN ERROR IDENTIFICATION: HAZOP AND TRACER-LITE COMPARED FOR THREE ATM SYSTEMS

EEC Note No. 08/03

Volume I

Project SRD-S-E1-0000 SAFBUILD

Issued: June 2003

REPORT DOCUMENTATION PAGE

Reference: EEC Note No. 08/03 – Volume I	**Security Classification:** Unclassified
Originator: EEC – SAS Safety Analysis & Science	**Originator (Corporate Author) Name/Location:** EUROCONTROL Experimental Centre Centre de Bois des Bordes B.P.15 F – 91222 Brétigny-sur-Orge CEDEX FRANCE Telephone : +33 (0)1 69 88 78 86
Sponsor: SAS	**Sponsor (Contract Authority) Name/Location:** EEC address as above

TITLE:

INDIVIDUAL AND GROUP APPROACHES TO HUMAN ERROR IDENTIFICATION: HAZOP AND TRACER-LITE COMPARED FOR THREE ATM SYSTEMS

Volume I

Author	**Date**	**Pages**	**Figures**	**Tables**	**Annex**	**References**
S. Shorrock (DNV – Det Norske Veritas)	06/2003	x + 40	4	9	1 (separate document)	27

	Project	**Task No. Sponsor**	**Period**
	SRD-S-E1-0000 SAFBUILD		2002 to 2003

Distribution Statement:
(a) Controlled by: Head of SAS
(b) Special Limitations: None
(c) Copy to NTIS: ~~YES~~ / NO

Descriptors (keywords):

Human error prediction – safety assessment – future ATM systems – CORA – Time-based separation – Co-Space

Abstract:

This report gives an overview of an independent comparison of two human error analysis techniques - HAZOP and TRACEr-lite - for three projects: Co-space, Time Based Separation and CORA 2. The report presents the high-level findings of the Co-space study and compares the performance of the techniques over all three applications. Example recommendations are provided for the projects and for the implementation of the techniques in EUROCONTROL. An Annex Note detailing all of the analysis, as well as the high-level findings for Time Based Separation and CORA 2, accompanies this main report.

FOREWORD

The principal safety component in current ATM is the controller. Given the future changes that are going to happen in ATM, controllers will be faced with new technology, new airspace concepts, and increased traffic levels. Each and all of these could lead to human errors that could potentially compromise ATM system safety. There is therefore a need for predicting such errors with future system concepts, designs, and working practices. Two human error analysis techniques were therefore identified and have been tested on three different EUROCONTROL projects, and both were found to work successfully, though with some differences in their scope and best time of application. Nevertheless, these two techniques now represent a good way forward for assessing human error potential in future systems, and for determining how to make future system designs more robust.

This main note therefore outlines the study and its conclusions, enabling the reader to see what the tools look like, and the type of output and insights they produce, and their relative advantages. A companion note (a technical annex) gives comprehensive detail from the study, and is intended more for the practitioner who wishes to see exactly what type of detailed output is produced by the application of these two techniques.

It is hoped that these techniques will be put to good use in the assessment of future projects, helping ultimately to ensure that the controller remains the principal safety ingredient in ATM safety.

Dr. Barry Kirwan
EEC Safety R&D Co-ordinator

CONTENTS

EXECUTIVE SUMMARY

EUROCONTROL commissioned DNV to perform an independent assessment and comparison of two approaches to 'human error analysis' that may support the process of designing for safety. The approaches selected were:

- **(Human) HAZOP** - a modification of an established, group-based approach to human hazard identification, based on the HAZOP study method developed in the chemical industry, focusing on safety-relevant human and information aspects, and
- **TRACEr-lite** - a relatively new, single analyst-led approach to human error analysis developed for ATM, analogous to the engineering-based 'Failure Modes and Effects Analysis'.

The findings of the study will be used to begin developing a 'portfolio' of complementary methodologies to help projects build safety into design.

The two methods were tested on three EUROCONTROL projects: **Co-space**, **Time-Based Separation (TBS), and CORA 2**. The study compares independently the two techniques (studies performed separately by two independent analysts) to show the kinds of insights to safety and design they can deliver, and to show the relative advantages of each for human error analysis purposes. The project does **not** attempt to provide a full safety assessment. Also, the results need to be considered in context. This study of HAZOP/TRACER has been a '*partial*' review of Co-space, TBS and CORA 2, and so has focused on potential errors but has not considered these concepts' respective safety benefits. This needs to be borne in mind when considering the numbers of errors identified and their individual severity. Such results are only useful for contrasting performance between TRACER and HAZOP, and are not reliable indicators of these projects' safety adequacy. For the latter, more complete and balanced study would be necessary.

Both techniques identified a wide variety of errors associated with tasks relevant to Co-space, TBS and CORA 2. TRACEr-lite was able to analyse a representative sample of controller tasks (nine or 10 for each project), and identified the majority of controller errors (approximately 91%) identified by HAZOP. HAZOP analysed one or two tasks for each project, and identified a smaller proportion (approximately 42%) of the controller errors identified by TRACEr-lite for the three projects. HAZOP did, however, address pilot errors and performance conditions. Also, HAZOP tended to concentrate on higher consequence errors, while TRACEr-lite looked at more errors with operability impacts. Both techniques elicited useful recommendations for the projects.

Both techniques were found to be of value to EUROCONTROL. The best way forward was considered to be a preliminary (Human) HAZOP to scope the critical tasks, and identify key errors, consequences and safeguards, followed by a detailed TRACEr-lite analysis later in the design lifecycle.

The following table shows the relative advantages and disadvantages of HAZOP and TRACEr-lite as found during this study, rated on a number of criteria from ★ to ★★★★★(best).

Criteria	HAZOP	TRACEr-lite
Comprehensiveness	★★★★ + Generally ensured that the 'big safety issues' were identified for the main tasks. + Identified other issues such as pilot errors and performance conditions. - Only a subset of tasks was analysed using HAZOP - Identified relatively few of the controller errors identified by TRACEr-lite (42%), though this does not account for criticality. - Less useful for operability issues (based on the project test cases – however in other settings has been found to be useful for operability issues).	★★★★★ + Provided a highly comprehensive and detailed 'register' of potential errors. + More tasks were analysed using TRACEr-lite in less time. + For the tasks analysed by HAZOP, TRACEr-lite identified most of the ATCO errors identified by HAZOP (91%). + For issues outside the scope of the TRACEr-lite analysis (e.g. pilot errors and general performance conditions), TRACEr-lite was able to predict some related errors. +/- Analysed errors in a more detail. - Detailed analysis can result in too much detail at the expense of the 'big picture'. - Focused on ATCO errors only.
Life cycle applicability	★★★★ + Can be used throughout the formative and summative phases of system design lifecycle. + Can be used at a high or low level of detail, depending on stage of development.	★★★ + Can be used throughout the formative and summative phases of system design lifecycle following concept selection. - Requires detailed task analysis.
Theoretical validity	★★ + Guidewords are developed from logical human performance outcomes. - Not based on a model of human performance.	★★★★ + Based on a model of human performance, with a theoretically plausible internal structure.
Operational validity (realism)	★★★★★ + Uses the expertise of the HAZOP team. This is an established method of ensuring that such analyses are contextually relevant.	★★★ + Uses project personnel to construct and review the Context Statement and Task Analysis. + Post-HEA review can add to context validity. -/+ Analyst may not be very knowledgeable about project. Some of the TRACEr-lite-predicted errors may appear somewhat 'naïve'.
Flexibility	★★★★ + Early in the concept development/selection process, a preliminary HAZOP can be performed, using the creative brainstorming and knowledge of the group.	★★★★ + Allows different levels of detail in the analysis and the analyst can employ different taxonomies. - Requires more developed task analysis
Usefulness (ability to improve safety)	★★★★★ + Helped to produce error reduction or mitigation measures. + Encourages the 'buy-in' of the project	★★★ + Helped to produce error reduction or mitigation measures. + Initial recommendations can be

Criteria	HAZOP	TRACEr-lite
	team and rapid incorporation of recommendations.	supplemented by project team following TRACEr-lite analysis. - Fewer recommendations generated. - Initial recommendations were not developed by project team.
Resource efficiency (training)	★★★ + Little or no training is required to act as a participant. - More extensive training is required in order to facilitate HAZOPs. - The role of the HAZOP leader may not suit every individual.	★★★★ + Training would normally take 1-2 days.
Resource efficiency (usage)	★★ - The need for a HAZOP team increases the number of person-days and it can be difficult to gather the whole team together for more than one day (~26.5 person days for a full analysis for all high-level controller tasks in the CORA 2 HTA).	★★★★ + TRACEr-lite is normally the more resource efficient technique (~16 days for a full analysis and reporting of controller errors for all high-level tasks in the CORA 2 HTA).
Usability	★★★★ + HAZOP has stood the test of time, and does not demand complex analysis from participants. - The process can prove arduous for participants, particularly where several unbroken days of analysis are performed.	★★★★ + TRACEr-lite is designed to be usable by non-HF specialists. - TRACEr-lite can be frustrating to the analyst due to the repetitive/exhaustive nature of analysis.
Auditability	★★★★★ + Provides a fully auditable process, with worksheets demonstrating the reasoning behind the analysis. + HAZOP visually projected each worksheet during the session so that all of the participants could verify the findings.	★★★★ + Provides a fully auditable process, with worksheets demonstrating the reasoning behind the analysis.

Recommendations for HAZOP and TRACEr-lite Implementation

The application of these two techniques to Co-space, TBS and CORA 2 produced the following recommendations for the future use of HAZOP and TRACEr-lite by EUROCONTROL:

1. For projects without detailed procedures or task descriptions, the preliminary HAZOP methodology is most appropriate for use by EUROCONTROL. This should identify the core tasks and critical, high-level errors, as well as the relevant safeguards and consequences. A detailed TRACEr-lite analysis should be conducted after the preliminary HAZOP, making use of the information derived from the HAZOP. For other projects with detailed task and system descriptions, the full HAZOP method may be used.

2. The HAZOP method can be modified to be used to assess Human-Machine Interfaces (e.g. Kennedy, et al., 2000). This variation of the

HAZOP approach would probably reflect more closely a TRACEr-lite analysis, and could be explored by project teams when interface design options are available.

3. In future sessions, there should always be a human factors specialist, safety specialist and a controller / pilot as a user representative on the HAZOP team.

4. A trained and experienced HAZOP leader should always lead the HAZOP session. It would also be beneficial where project teams have not used HAZOP before to have a short training session prior to commencing the project.

5. Full HAZOP sessions should be no shorter than 2 days, and normally 3-5 days. Preliminary HAZOPs for scoping purposes may be performed over one day in order to provide a high-level *identification* of the potential errors associated with a project.

6. One area of concern is the identification and implementation of appropriate safeguards or recommendations. Safeguards must be currently available or formally planned. Due to the integrated nature of EUROCONTROL projects, reliance is often placed on processes and technology that are also under development but outside the scope of the project. Care needs to be taken that lessons learned from one project are shared and/or incorporated into other projects and that the documented safeguards and recommendations are carried through to the operational phase of the project where appropriate.

7. Hierarchical Task Analysis should be performed using an easy-to-use, automatic hierarchical drawing package, able to export the associated text to Rich Text Format.

8. The use of TRACEr-lite's Internal Error Mechanisms is not necessary for the general TRACEr-lite analysis since the value of using error mechanisms is not justified by the analytical effort. However, they may be useful after the general analysis to examine the psychological causes of errors that are of high frequency, high severity, or low Recovery Success Likelihood (RSL).

9. Human error likelihood and criticality should be rated in future TRACEr-lite analyses in conjunction with the project teams, including operational specialists. The suitability of any risk ranking method needs to be considered carefully before us in HAZOPs.

10. The output of the error analysis should be reviewed by members of the project team including operational specialists, prior to formulation of recommendations and write-up.

1. INTRODUCTION

1.1 Background to the Study

Air Traffic Management (ATM) is in a period of major change, with a variety of new concepts under consideration to help air traffic controllers cope with projected increases in traffic levels. New technology has enabled considerable changes to current methods of operation, and automation is now widely acknowledged to be perhaps the only way to meet future capacity demands. Computer support and automation in aviation have been subject to increasing investigation and analysis over recent years. One of the key issues that has arisen from these studies is the effect that technology might have on 'human error'. 'Human error reduction' was once seen as a natural consequence of automation, but this premise was questioned (Wiener and Curry, 1980), and the real situation is being revealed. On the basis of experimental studies and operational experience, many commentators asserted that computers, and automation in particular, produce new error forms (Wiener, 1988; Sarter and Woods, 1995b). The occurrence of more frequent small errors in a non-automated system may be replaced by an automated system which has fewer, but larger errors, each with more significant consequences (Weiner, 1985, Billings, 1988). 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). Whatever the case, it is clear that these potential effects need to be managed.

EUROCONTROL have developed a Safety Assessment Methodology (SAM) as part of ESARR 4. This provides a robust methodology with which to conduct safety assessments, comprising a Functional Hazard Analysis (FHA), Preliminary System Safety Analysis (PSSA), and System Safety Assessment (SSA). These methodologies represent periodic checks on safety, from the early conceptual stage of a project, to the pre-operational stage. However, the methodologies may need to be supplemented with other techniques in order to provide a more fully integrated approach to 'designing for safety', and to better consider human involvements.

Various means exist to assist in this process. One approach called 'Human Error Analysis' (HEA) has seen increasing use since the 1980s. HEA methods involve two types of approaches. First, *group-based* approaches utilise a varied team of individuals to help brainstorm and analyse potential 'failures'. These approaches stem from the Hazard and Operability (HAZOP) and 'What-if' query-based methods. Second, *analyst-led* approaches generally utilise a task analysis and a classification system to probe potential errors and their psychological and contextual origins. These approaches stem from Failure Modes and Effects Analysis (FMEA), and include SHERPA (Embrey, 1986), CREAM (Hollnagel, 1998) and TRACEr (Shorrock and Kirwan, 1999, 2002).

EUROCONTROL led a study to test independently two HEA approaches for 'human error analysis' that may support the process of designing for safety. The approaches selected were:

- **(Human) HAZOP** - an established, group-based approach to human hazard identification based on the HAZOP study method, developed in the chemical industry.
- **TRACEr-lite** - a relatively new, single analyst-led approach to human error analysis developed for ATM.

The findings of the study will be used to begin developing a 'portfolio' of alternative methodologies for use on EUROCONTROL projects, particularly design projects and concepts studies.

The independent comparison of the two methods involved two separate analysts leading separate analyses of three EUROCONTROL projects, as described Section 1.2.

1.2 Test Projects

The three test EEC Projects are **Co-space**, **Time-Based Separation** and **CORA 2**. These projects are described briefly below.

1.2.1 Co-space

The Co-space project aims to increase controller availability though a reorganisation of tasks between controller and pilot and thereby achieve a more effective task distribution that is beneficial to all parties[1]. It is expected that increased controller availability could lead to improvements in safety, efficiency and/or capacity. Delegation of the aircraft spacing task from the controller to the flight crew is envisaged as a possible option to help achieve this. For aircraft within an aircraft arrival stream, the delegation could consist of tasking the flight crew to maintain a given spacing value to a lead aircraft, as defined by the controller.

Spacing tasks are delegated to flight crews upon controller initiative. The controller decides to delegate if appropriate and helpful. The delegation is limited since the controller can only delegate 'low-level' tasks (monitoring and implementation) as opposed to 'high-level' tasks (conflict detection and resolution). The delegation is flexible since the controller has the ability to select for each situation the level of task to be delegated from monitoring up to implementation. The delegation takes advantage of emerging technologies in pre-operational state along with additional avionics such as Cockpit Display of Traffic Information (CDTI) or an Airborne Separation Assistance System (ASAS). This project focuses on near-term applications taking place in current ATC organisations for both en-route airspace and terminal areas.

In the scope of defining a new task distribution between controllers and flight crews, from the onset of the project, two key constraints

[1] See www.eurocontrol.fr/projects/freer/publications.htm for a list of relevant publications.

were identified and adopted. The first one is related to human aspects and can be summarised by 'minimise change in current roles and working methods of controllers and flight crews'. The second one is related to technology and can be expressed as 'keep it simple as possible'.

The project is well established and has just completed a third cycle of user simulations. A set of delegation procedures exists and was used as the basis for analysis by HAZOP and TRACEr-lite.

1.2.2 Time Based Separation

The Time-Based Separation (hereafter referred to as 'TBS') project aims to define and investigate the relevance of a new concept of operation applied to the arrival phase of flights. This concept involves replacing actual distance based separations with time intervals.

More specifically, the project will investigate the possibilities of preventing loss of runway capacity under strong wind conditions while maintaining required levels of safety performance. The project will:

- Assess a new concept of separation based on time interval as opposed to Radar or ICAO Wake Vortex separation criteria.
- Investigate the use of lateral separations of less than 3 NM (or less than 2.5 NM if this is in use).
- Explore possibilities of compensation of wind effect by aircraft speed adjustment and required ATC techniques.

This project is in the very early stages of background research and concept development, with no outline procedures at the time of the study.

1.2.3 CORA 2

The Conflict Resolution Assistant (CORA) provides computer-based support for air traffic controllers in the detection, identification, prioritisation and resolution of predicted conflicts in the en-route flight phase. Conflict identification and resolution is a core ATC task today, carried out by Planner Controllers (longer-range) and Tactical Controllers (shorter-range) by scanning the radar display and paper or electronic strips. Without change, increased traffic will naturally bring more conflicts, leading in turn to higher workload for controllers and more complex conflict resolution problems. CORA aims to improve planning and anticipation processes through earlier conflict notification and resolution decisions with the introduction of new computer-based ATM, and the associated evolution of ATC procedures, roles, tasks and working methods. This improvement should also help to smooth peaks in controller activity, redistribute workload between Planner and Tactical Controllers, and improve level and quality of service for airlines by minimising deviation from airline optimal trajectories via earlier and more strategic resolutions.

The 'CORA 1' system will identify conflicts for controllers and support the planning and decision making process by helping to test the impact of tactical clearances on the traffic situation. 'CORA 2' will provide a set of ranked, conflict-free resolution advisories for the controller, who can directly select and implement one of the suggested advisories, or employ a different, self-generated resolution. The CORA 2 project is defining and developing operational requirements and prototype enhanced concepts for conflict resolution.

1.3 Objectives

The aim of the project was to apply the techniques TRACEr-lite and HAZOP to representative projects in three areas to assess the relevance of the techniques, showing what they can deliver in terms of safety and design insight, and showing the relative advantages of each for human error analysis purposes. It was not an objective of the study to perform a safety assessment, but rather to provide an illustration of the potential analyses that could be performed, and their added value to safety.

1.4 Report Structure

The remaining sections of this report are structured as follows:

- Section 2 of this report provides a description of the HAZOP study method.
- Section 3 describes the TRACEr-lite method.
- Section 4 provides an overview of the Co-space study, including the HAZOP and TRACEr-lite approach, comparison of results, discussion and recommendations.
- Section 5 contains a discussion of the study, including a comparison of HAZOP and TRACEr-lite on a number of criteria.
- Section 6 suggestions a number of recommendations for the implementation of HAZOP and TRACEr-lite in EUROCONTROL.
- Section 7 states the main conclusions of the study.
- Section 8 contains References.

A separate Annex report accompanies this report, and contains the detailed HAZOP logsheets, Hierarchical Task Analyses (HTAs) and TRACEr-lite analyses for Co-space, Time-Based Separation and CORA 2, as well as overviews of the Time-Based Separation and CORA 2 studies.

2. HAZOP DESCRIPTION[2]

2.1 Introduction to HAZOP

Hazard and Operability (HAZOP) studies provide a formal, systematic and critical examination of the process and engineering intentions of a design (see Kletz, 1999). HAZOP examines the potential for hazard and identifies mal-operation or malfunction of individual items of equipment and the consequences for the whole system. This examination of the design is structured around a set of guidewords, which ensure complete coverage of all possible problems. HAZOP studies normally involve a team who have experience of the system or design to be studied.

HAZOP studies normally involve a team who have experience of the system or design to be studied, including design, engineering and operational personnel, often also including training specialists, human factors specialists, and independent safety specialists. These team members apply their experience of the design and their technical expertise in the HAZOP study sessions to achieve the aims of the HAZOP.

Each HAZOP has a set of objectives, which are particular to that study and which are decided as near to the beginning of the study as possible. However, there are four overall aims to which any HAZOP should be addressed:

- To identify all deviations from the way the design is expected to work; their causes, and all the hazards and operability problems associated with these deviations.
- To decide whether action is required to control the hazard, or the operability problem, and if so to identify the ways in which the problem can be solved.
- To identify cases where a decision cannot be made immediately and to decide on what information or action is required.
- To ensure that actions decided upon are followed through.

2.2 The Use of Guidewords

HAZOP methodology was developed by ICI in the United Kingdom during the 1970s. Early in that decade ICI decided that they required a more formalised technique for critical analysis of plant design. They had reviewed the techniques being used in various parts of the company, and concluded that their quality was too heavily dependent on the people who made up the study teams.

Over several years, Method Study experts in the company devised and applied a formal review technique. This included a set of guidewords, which were later adapted to be usable by a wider range of

[2] Further details of the HAZOP method can be obtained from the EUROCONTROL Contact Person indicated on Page ii of this report.

people, including definitions, as shown in Table 1. The guidewords in the table are used to consider each applicable process variable, etc., and to develop scenarios, which could lead to hazards or operability problems.

Table 1: Summary of HAZOP Guidewords with Explanations of Their Meaning

Guidewords	Meanings	Comments
NO, NOT OR NONE	The complete negation of the design intention	No part of the intentions is achieved and nothing else happens
MORE OF LESS OF	Quantitative increase/ decrease of any relevant physical parameters	These refer to quantities and relevant physical properties such as flow rates and temperatures as well as activities like “HEAT” and “REACTION”
AS WELL AS	A qualitative increase	All the design and operating intentions are achieved together with some additional activity
PART OF	A qualitative decrease	Only some of the intentions are achieved; some are not
REVERSE	The logical opposite the intention	This is mostly applicable to activities for example, reverse flow or chemical reaction
OTHER THAN	Complete substitution	No part of the original intention is achieved. Something quite different happens

2.3 HAZOP Method for Human Hazards

The HAZOP study method can also be applied to the study of a task, human-machine interface or operating procedure (see Livingston, 2001; Kennedy et al, 2000). A ‘task’ can be seen as a set of things including a system goal, resources for accomplishing the system goal, including information and controls and a set of constraints on how the goal may be achieved using these resources (Shepherd, 2001). A ‘procedure’, meanwhile, is defined here as a set of instructions whose aim is to direct an operator to make changes to the state of a system in a safe manner, so that a particular objective is achieved.

When studying a task or procedure, the hardware itself is not studied in detail, but normally it would have already been the subject of a HAZOP study, or would be reviewed subsequently if designs were not available. If a previous study has been conducted, the team studying the task or procedure should be aware of this. The team will first identify the intent of the task or procedure. In broad terms this requires that the team understand the system state at the beginning of the task/procedure, and the required system state at the end. The HAZOP team will also need to know how the task/procedure will be achieved.

The team is ready to begin the detailed study when the intent is clear. This is carried out in a step-by-step manner and for each individual task or procedure step the team agree an objective or intent. They will then view the step as requiring an action at a time in a sequence. If procedural documentation is available, they will also review the wording of the instruction. For completeness, the team may consider additional concepts, including clarity, unattended operation, training, purpose, abnormal conditions and maintenance.

It is thus possible to generate special guidewords focussing on human and information issues, using the ‘original’ set in Table 1, with some key human parameters (e.g. Action, Time, Sequence, Information), and some additional concepts. A set of guidewords and associated meanings is shown in Table 2.

Table 2: (Human) HAZOP Guidewords and Issues

Guideword	Meaning
Purpose	Is the task step needed? - is the intent of this step clear? - can this step be mis-applied?
No action	Task step is missed or omitted - intended operation did not occur (mechanical failure) - action impossible - equipment not ready (locked out, not in service).
More action	Operator does more than intended - other actions occur.
Less action	Operator does less than intended - equipment does not perform as required - not enough time to complete the step.
Wrong action	Operator performs the wrong action, operates the wrong equipment, reads the wrong instrument - performs different or out of date procedure - performs two or more steps at the same time.
Part of action	Operator only completes part of a composite action (misses out middle part, or final part).
Extra action	Operator assumes s/he is required to do something in addition to what is specified - other procedures interfering - other personnel in wrong area - poor communication (operation, maintenance, engineers, etc.).
Other action	Operator misunderstands instruction and does something completely different - remembers a similar procedure and follows that instead.
More time	Operator takes longer than necessary over action, (e.g. gets distracted) - starts next action later than expected.
Less time	Operator carries out action too quickly - starts next action earlier than expected.
Out of sequence	Operator misses out a step - carries out a step before it should occur, or after it should occur.
More information	Procedure or HMI includes information that is unnecessary and could lead to confusion - contains information that contradicts other information.
Less information	Necessary information is missing from the procedure or HMI - especially information about the starting condition - information which allows operator to check progress, or to identify errors and correct.
No information	No feedback from the system - procedure does not specify expected performance - no specified actions for emergencies.
Wrong information	Information provided is wrong, out of date - contradiction (oral instruction vs. written, other procedures or steps within this procedure).
Clarity	Step or verbiage confusing or complex - readability - poor procedure layout.
Training	Adequate training - is certification required and provided for this step? - procedure control (issuing, updating, revisions, overriding, communication, distribution/acknowledgement, retraining).
Abnormal conditions	Emergencies - recovery from abnormal situations - utility failure severe or unusual weather - deviation from procedure - makeshift operations.
Maintenance	Work permits required - equipment condition - recalibrations - interface with operations.
Safety	Personnel protection - Regulation compliance - environmental considerations - electrical hazard, etc.

2.4 Preliminary Study Method

The detailed method for study of procedures is time consuming but thorough. Therefore, it can be inefficient to follow the full HAZOP method if the task or procedure is under-developed. For a new procedure, or one that has not been reviewed for some time, a two-stage process may be preferable.

In the two-stage process a preliminary study is carried out first, using a short parameter list, combined with guidewords where necessary. Later, when the task or procedure is more developed, a full study is performed. The preliminary study is normally carried out by a small team of 3 or 4 people, including representatives from operations and process technology. The parameters used are often as follows:

- Purpose
- (No) Action
- (More) Time
- (Less) Information

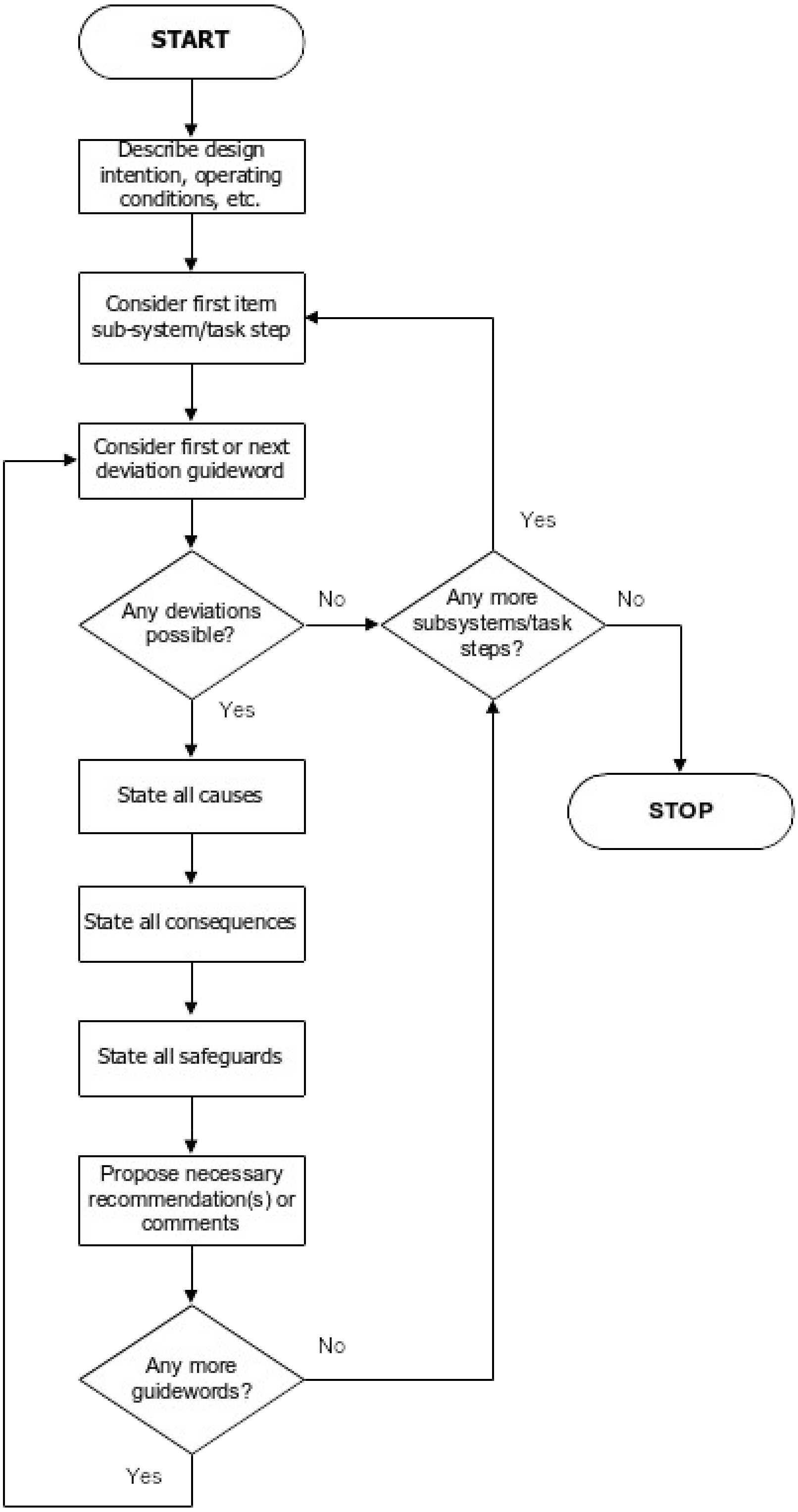
For Action, Time, and Information parameters, the team would start with, for example, No Action, but would not necessarily limit themselves to ‘No’. This shortened process may generate a procedure which needs little further change as a result of the fully study process.

2.5 Undertaking the Study

A study meeting will follow through a series of steps repeatedly. There are several stages that are repeated many times during a HAZOP, as in Figure 1. At the beginning of the first study session, the team leader invites the lead engineer to outline the design intentions as a whole in very broad terms. This ensures that each team member has an adequate knowledge of the system and the way sections operate within the overall design. At the beginning of the study of each section of the system, the team leader asks for a statement of the design intention of this section in greater detail, including information on operating parameters within the section.

HAZOP sessions are structured with the team leader facilitating the discussion. The guidewords are applied by the team leader, stimulating discussions about likely deviations. The team is then encouraged to discuss the causes, consequence and possible actions for each deviation. As hazards are detected, the study leader ensures that everyone understands them, and that they are properly recorded in a HAZOP table.

Figure 1: Process for carrying out a HAZOP Study



2.6 Recording the Results

For any study involving the HAZOP technique, it is important to record all hazards, questions or operating/maintenance problems identified for the attention of project management. By this means, follow-up work may be accurately monitored as the design work proceeds. The results are recorded on a log sheet by a secretary or recorder, who details tasks, deviation guidewords, causes, consequences, safeguards, risk ranking (if used) and recommendations.

A HAZOP is normally documented by "recording by exception", i.e. only recording the deviations which cause particular hazards or operating problems. In this way, the amount of documentation can be kept at a reasonable level. The study findings are recorded on HAZOP worksheets. An extract of a worksheet (for Co-space) is shown in Table 3.

The HAZOP study is completed to draft report stage, by the issue of a report summarising the study, and giving a specific list of recommendations, together with the worksheets on which the outcome of group discussion is recorded. The study is completed by the issue of a final report, giving details of follow-up actions.

2.7 Risk Ranking of Consequences

In some studies it is appropriate to use a qualitative risk-ranking matrix to assign a level of severity and likelihood of occurrence of the identified consequences (e.g. as provided in ESARR4). The process of judging hazard likelihood and severity can, however, be problematic in ATM and is not discussed further here.

2.8 Requirements for Recommendations

When the HAZOP team feels that the safeguards are inadequate in light of the risk imposed (combination of likelihood of occurrence and severity of consequences), a specific recommendation is made. The team must be confident that if the recommendation is carried out it will either remove the problem or reduce probability or consequence to an acceptable level without introducing new problems. The recommendations generated by the HAZOP team may be changes to the HMI, task design, working environment, written procedure, training, equipment, etc.

If the team is in doubt about whether or not any action is required or what that action should be, they should record a recommendation for further study. Such a recommendation should specify clearly the problem and the scope and objectives of the required study.

Table 3: Extract of HAZOP worksheet for Co-space.

Project: Co-space, Delegation of "Merge Behind"			Subsystem 1: Identify and Select Target				Recommendations
Guideword deviation	**Error / Causes**	**Consequences**	**Risk Ranking**			**Safeguards**	
			S	**L**	**R**		
2. Wrong action	2.1. Controller identifies wrong target	2.1. Potential for aircraft collision	3	4	U[3]	2.1. Target positioning by pilot	1. Anti Overlap (display decluttering) as it currently exists needs some improvement. Review how this software tool can be used to support the controller during delegation and what improvements are required for it to be effective.
						2.2. Confirmation of target	2. Consider making target positioning by pilot a compulsory subtask in target selection.[4]
						2.3. Read back of target from pilot to controller	3. Explore how data link technology could be used to support both controller and pilot when selecting a target during delegation.
						2.4. The pilot may question the target selection if he has enough supporting information	
						2.5. Controller monitoring of the aircraft may identify that the pilot has the wrong target later in the task.	
						2.6. The pilot's TCAS (visual and audible alarm)	
						2.7. The controller's STCA (short term conflict alert) will sound a couple of minutes before separation infringement	
						2.8. The use of Anti-Overlap software tool on the controller's interface	

[3] A Risk ranking value [R] of 'U' means 'Unacceptable', i.e. that the situation should be changed to improve safety – this is illustrative only here.

[4] This had been identified by the project team prior to the HAZOP, but the HAZOP confirmed its utility.

3. TRACER-LITE DESCRIPTION[5]

3.1 Introduction to TRACEr-lite

TRACEr (Technique for the Retrospective and Predictive Analysis of Cognitive Errors) (Shorrock and Kirwan, 1999, 2002) was developed from research findings and operational experience for predictive and retrospective human error analysis in ATM. TRACEr comprises a set of decision-flow diagrams and tables containing human error modes and mechanisms, and associated taxonomies, intended for use by human factors specialists[6]. TRACEr has been applied to a number of ATM projects, retrospectively and predictively. In its predictive mode, TRACEr was applied in the UK to a new ATM situation display, electronic flight strips and some new controller tools (Shorrock, et al, 2001), a final Approach Spacing Tool for use by Heathrow Approach Control (Evans et al, 1999), and to reduced separation minima in unregulated airspace (Shorrock and Kirwan, 2002). These trial applications delivered useful insights for the projects, and led to new design decisions that were implemented. Significantly, a significant number of the predicted errors were observed in subsequent simulations and trials, thus providing an indication of good predictive validity[7].

Whilst these early studies were encouraging, it was realised that for the potential of TRACEr to be realised more fully, a simpler, reduced-scope version was required. This version of the technique was called 'TRACEr-lite' (Shorrock, 2002a, b).

For predictive use of TRACEr-lite, the analyst first scopes the analysis, and then conducts a task analysis, e.g. using Hierarchical Task Analysis (HTA) (see Shepherd, 2001). Using TRACEr-lite and the task analysis, the analyst determines what could go wrong. There are four key components to the TRACEr-lite toolkit (see Figure 2).

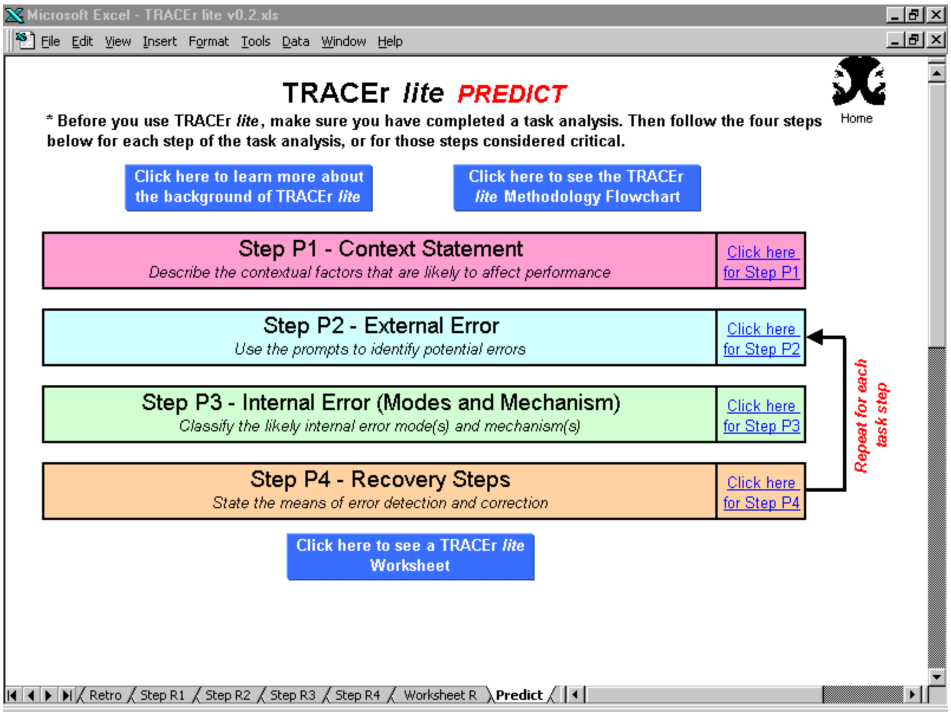
---

[5] Further details of the HAZOP method can be obtained from the EUROCONTROL Contact Person indicated on Page ii of this report. TRACEr-lite is non-proprietary and will be available freely on the internet at www.TRACEr-lite.co.uk in the near future.

[6] TRACEr was adapted for retrospective use in Europe in the EUROCONTROL 'HERA' project - human error in ATM (see Isaac, et al., 2002), which, in collaboration with the Federal Aviation Administration (FAA), was further developed in a joint project resulting in the HERA-Janus technique.

[7] In one application, 92% of the errors that were observed during extensive observations of simulations sessions were previously predicted by TRACEr. Those errors that were not predicted were not represented in the associated task analysis.

Figure 2: TRACEr-lite light prototype interface and predictive task steps.



3.2 Step P1 - Context Statement

Prior to the TRACEr-lite analysis, during the task analysis process, Performance Shaping Factors (PSFs) are analysed to set the scene for the analysis. PSFs are those factors, either internal to the controller or pilot, or relating to the task and operational environment, that affect performance positively or negatively, directly or indirectly. The PSFs are used to prepare a general 'Context Statement'. This is a set of statements about the performance conditions under which the controller will be working. PSFs may also be analysed separately for particular task steps, relating to specific errors, if the analyst so chooses. Each PSF takes the form of a question, eliciting a 'yes'/'no' response and a statement of justification. These questions occupy eight categories, such as traffic and airspace, procedures and documentation, training and experience, workspace design/HMI/equipment, etc. TRACEr-lite does not predetermine the links between PSFs and error modes/mechanisms because of the many-to-many mapping relationships involved, as well as the uncertainty in making such specific links. However, some general guidance is provided on how particular types of PSF affect cognitive processing.

3.3 Step P2 - External Error (Modes)

Once a context statement is prepared the analyst engages in a cycle of activities, applying the TRACEr-lite taxonomies to the detailed task steps within the task analysis. External Error Modes (EEMs) are first used as prompts to enable the identification of the observable manifestations of potential errors, based on logical outcomes of erroneous actions, in terms of timing, sequence, selection and quality. Examples include ‘Omission’, ‘Wrong action on right object’, ‘Mis-ordering’, and ‘Information not sought / obtained’. EEMs are context-free and independent of cognitive processes (e.g. intention). However, when used on a task step from a task analysis, the error mode is converted to a contextual ‘external error’. Hence, when the EEM ‘Omission’ is combined with the task step ‘Issue instruction to select unpositioned target’, the external error recorded becomes ‘Controller fails to issue instruction to select unpositioned target’.

3.4 Step P3 - Internal Error (Error Modes and Mechanisms)

The cognitive aspects of the error are analysed using a set of Internal Error Modes and Mechanisms. These are structured around four error domains, with an associated question prompting further classification:

- **Perception** - Does the controller/pilot have to see or hear something during the task step?
- **Memory** - Does the controller/pilot have to recall information or remember to perform actions in the future during the task step?
- **Decision making** - Does the controller/pilot have to project required separation, or make a plan or decision during the task step?
- **Action** - Does the controller/pilot have to perform a manual action or say something during the task step?

Internal Error Modes describe how the controller’s/pilot’s performance failed to achieve the desired result. One or more Internal Error Mode is used for each error identified in the report. For instance, Internal Error Modes within the ‘Perception’ error domain include ‘mishear’, ‘mis-see’, ‘no detection (visual)’ and ‘no detection (auditory)’. TRACEr-lite contains 14 error modes - three or four for each domain.

Internal Error Mechanisms describe in greater depth the psychological underpinnings of an Internal Error Mode. TRACEr-lite contains 19 error mechanisms - four or five for each domain. Example error mechanisms within the ‘Perception’ domain include ‘expectation’, ‘confusion’, ‘discrimination failure’, ‘perceptual overload’ and ‘distraction/preoccupation’. The TRACEr-lite error modes and mechanisms are shown in Table 4.

Error mechanisms can better enable the consideration of measures to reduce or mitigate errors, because the internal cause of the error can be analysed. For example, if a controller could misidentify an aircraft on radar, this may be due to ‘confusion’ (e.g. visually similar callsigns). Such errors could lead to attempts to increase the distinctiveness of lettering, and in the meantime raise awareness of the issue with controllers. However, the error may occur due to ‘perceptual overload’ (e.g. a lot of traffic information on radar). These types of errors may lead to attempts to filter the amount of information displayed, split the sector, etc. If the ‘internal cause’ (error mechanism) is not understood, an inefficient error reduction strategy may be implemented.

Table 4: TRACEr-lite Internal Error (Modes and Mechanisms) taxonomy

Error Mode	Error Mechanism
Perception	
Mishear	Expectation
Mis-see	Confusion
No detection (auditory)	Discrimination failure
No detection (visual)	Perceptual overload
	Distraction / Preoccupation
Memory	
Forget action	Confusion
Forget information	Memory overload
Misrecall information	Insufficient learning
	Distraction / Preoccupation
Decision Making	
Misprojection	Misinterpretation
Poor decision or poor plan	Failure to consider side- or long-term effects
Late decision or late plan	Mind set / Assumption
No decision or no plan	Knowledge problem
	Decision overload
Action	
Selection error	Variability
Unclear information	Confusion
Incorrect information	Intrusion
	Distraction / Preoccupation
	Other slip

Following the analysis of Internal Errors, **Initial Consequences** are determined by a process of analysis. Consequences are stated as free text, and are normally restricted to the more immediate and likely effects and consequences. Error likelihood and severity are not rated as part of the standard TRACEr-lite approach, but can be rated by a team of individuals if appropriate, for instance using data (e.g. simulation-derived), or expert judgement.

3.5 Step P4 - Recovery Analysis

The next step in the TRACEr-lite process involves considering **Recovery** from the error. This may involve stating a future step in the task analysis, or stating the 'detection means', i.e. cues from the work context, e.g. RT readback, radar monitoring, other controller, etc. The analyst may also at this point rate the 'Recovery Success Likelihood (RSL)'. This is a subjectively rated likelihood of recovering the task successfully without adverse consequences, assisted by the use of an anchored rating scale contained within TRACEr-lite.

On the basis of this analysis, **Comments** or **Questions** may be made or **Recommendations** may be proposed. However, rather than propose recommendations in a reactive fashion, these are normally proposed during the synthesis of the data to try to ensure that common themes that are identified can be addressed with a manageable set of recommendations or requirements. The process above is illustrated in Figure 3. An example of TRACEr-lite analysis output is shown in Table 5.

Figure 3: Process of Using TRACEr-lite

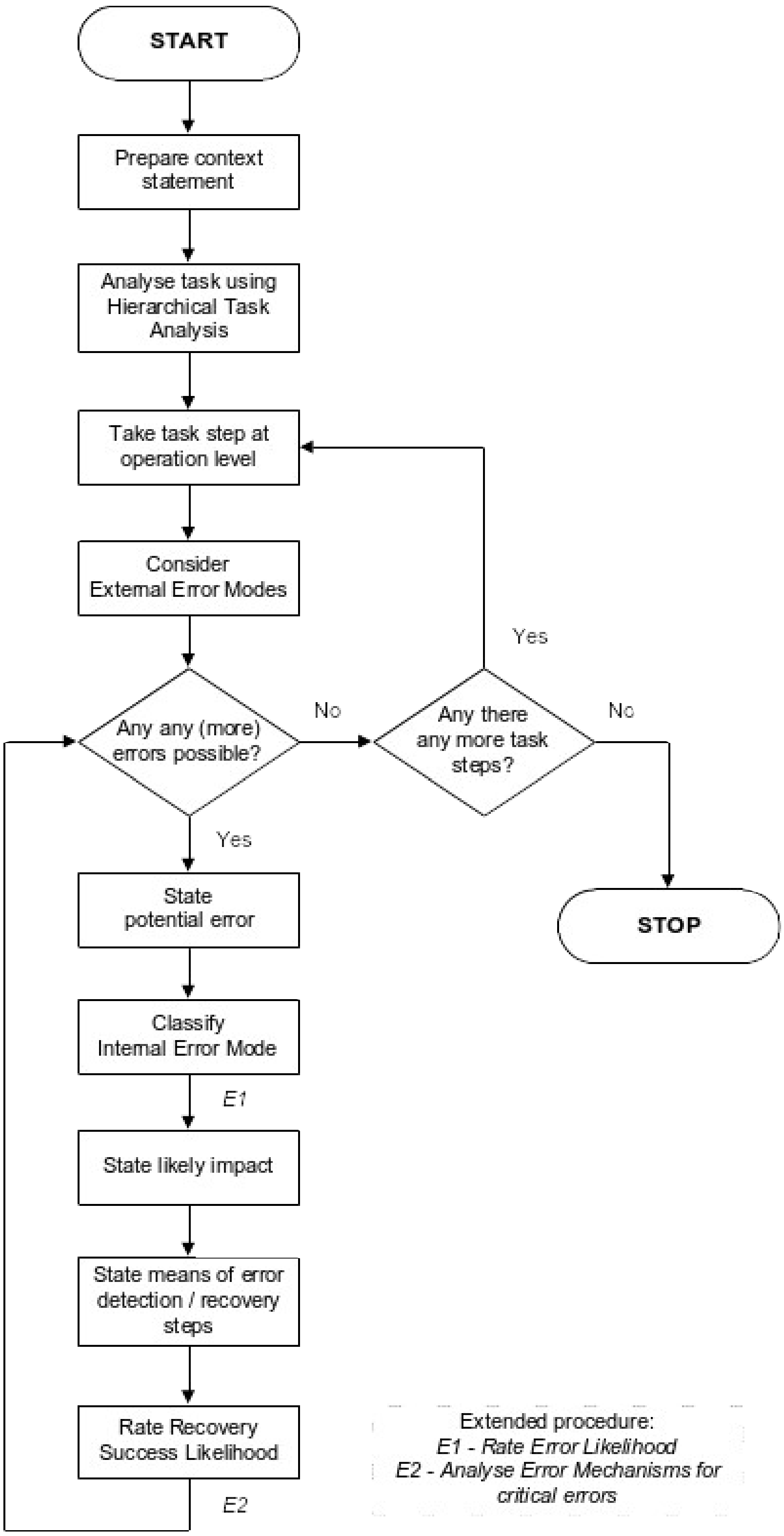


Table 5: Extract of TRACEr-lite analysis worksheet for Co-space[8].

Task Step	External Error	Internal Error	Initial Consequences	Detection Means	RSL
1.5 Conduct Identification Phase	↓				
Do 1, 2, 3 or 4 as required. Then do 5 if required. Then do 6 if required.					
1.5.1 Instruct pilot to select unpositioned target	↓				
Do 1 to 4 in order. Then do 5 or 6. Do 7 throughout as appropriate.					
1.5.1.1 Issue instruction to select unpositioned target ||	1. Fail to issue instruction to select target 2. Instruct pilot to select wrong target 3. Issue wrong / inappropriate instruction 4. Issue instruction to wrong aircraft 5. Issue unclear instruction	1. (M) Forget action 2, 4. (A) Incorrect information, Unclear information 3. (D) Misprojection, Poor decision; (A) Incorrect information 5. Unclear information	1. Pilot does not select target; No delegation; Pilot selects target late; Applicability conditions may change 2. Pilot tries to select wrong target 3. (Depends on instruction) Pilot responds to instruction (select / position) 4. Wrong aircraft selects target 5. Pilot tries to select wrong target; Pilot does not select target; Pilot selects target late	1. Memory 2, 5. RT readback 3. Radar monitoring; RT readback 4. RT readback; Radar monitoring	1. M 2. M-H 3. H 4. M-H 5. M
1.5.1.2 Receive pilot readback for selecting target ||	1. Fail to detect / query erroneous readback 2. Fail to detect / query missing readback	1. (P) Mishear 2. (P) No detection - auditory; (M) Forget action; (D) Poor decision, No decision	1, 2. Pilot may have selected wrong target aircraft	1. Radar monitoring	1. L-M 2. M

[8] 'Comments' column not shown in this extract.

4. CO-SPACE STUDY OVERVIEW[9]

The first stage of data collection for both HAZOP and TRACEr-lite comprised an initial scoping meeting with the Co-space project manager, project human factors specialist, and an operational specialist (air traffic controller). During this meeting, the concept was presented to the HAZOP leader and the TRACEr-lite analyst. The Co-space project was in a relatively advanced stage, with a concept developed and procedures being tested in real-time simulations.

It was established in this meeting that the delegation process comprises three phases:

- **Phase 1: Identification phase** - the controller indicates the target aircraft to the pilot of the delegated aircraft.
- **Phase 2: Instruction of delegation** - the controller specifies the task to be delegated to the pilot.
- **Phase 3: End of delegation** - the completion of the task delegated to the pilot.

There are four possible delegation scenarios: ‘Remain behind’, ‘Heading then remain behind’, ‘Merge behind’, and ‘Heading then merge behind’.

4.1 HAZOP Approach

The HAZOP study for Co-space proceeded according to the methodology described in Section 2. Since the Co-space project is addressing the delegation of spacing from the controller to the flight crew, the HAZOP looked at one of the four possible scenarios for delegation: “Merge Behind”. For this task the two aircraft are flying merging trajectories in cruise or in descent and the desired spacing is obtained at the merging point. The HAZOP considered both controller- and pilot-related errors, since all were judged relevant and useful to consider while each delegation phase was being considered.

Due to restrictions in the project team’s availability, two half-day sessions were held at the EEC in Brétigny on the afternoon of Thursday 17th October 2002 and the morning of Friday 18th October 2002. The HAZOP sessions were attended by three project team members including a human factors specialist and an air traffic controller. The sessions were facilitated by a human factors specialist/engineer, and recorded by an avionics engineer. In the time available (approximately one day), it was only possible to cover Phase 1 and Phase 2 for the scenario “Merge Behind”.

Where possible a risk matrix adapted specifically for the study was used to rank the likelihood and severity of the consequences (see Annex).

[9] This Main Report provides an overview of only the Co-space findings. Overviews of the TBS and CORA 2 findings are provided in the Annex report.

4.2 TRACEr-lite Approach

The TRACEr-lite study for Co-space proceeded according to the methodology described in Section 3. The TRACEr-lite analysis began with the development of a Hierarchical Task Analysis (HTA) of the delegation process. However, since Co-space has implications for other tasks (such as takeover/handover and spacing monitoring), it was decided to represent the range of tasks of the Extended TMA controller using Co-space.

Following the initial consultation and during the task analysis process, various documents were reviewed, as follows:

- EUROCONTROL (2001). *Freer Flight: Evolutionary Air-Ground Co-operative ATM Concepts (EACAC). Procedures of Delegation of Separation from the Controller to the Flight Crew*. Version 2.2. Issued 13 November 2001. (This contains procedures and RT protocol.)
- EUROCONTROL (2002). *CoSpace Real-Time Experiment Briefing Document*. Version 1.1. Issued 07 November 2002. (This contains delegation interface diagrams.)
- Co-space conference publications (various, available on www.eurocontrol.fr/projects/freer/publications.htm).

Because draft procedures were available, it was possible to represent the task steps in some detail in an HTA. The draft HTA was presented to each of the project team individually during a second set of data collection meetings with the same three project personnel, each lasting one to two hours. Each project team member helped to shape and modify the HTA until an agreed version was formed. Following these interviews, the controller interface diagrams were examined and the associated controller interactions were added to the 'low-level' tasks of the HTA. Following the meeting, the TRACEr-lite analyst sent the finished HTA to the meeting attendees for review and comment.

A representative HTA for controller tasks related to the implementation of Co-space is presented in Appendix A.10, contained in the Annex to this report. The HTA was constructed for the range of tasks for the Extended Terminal Manoeuvring Area (ETMA). The HTA 'top-level' tasks are shown in Table 6.

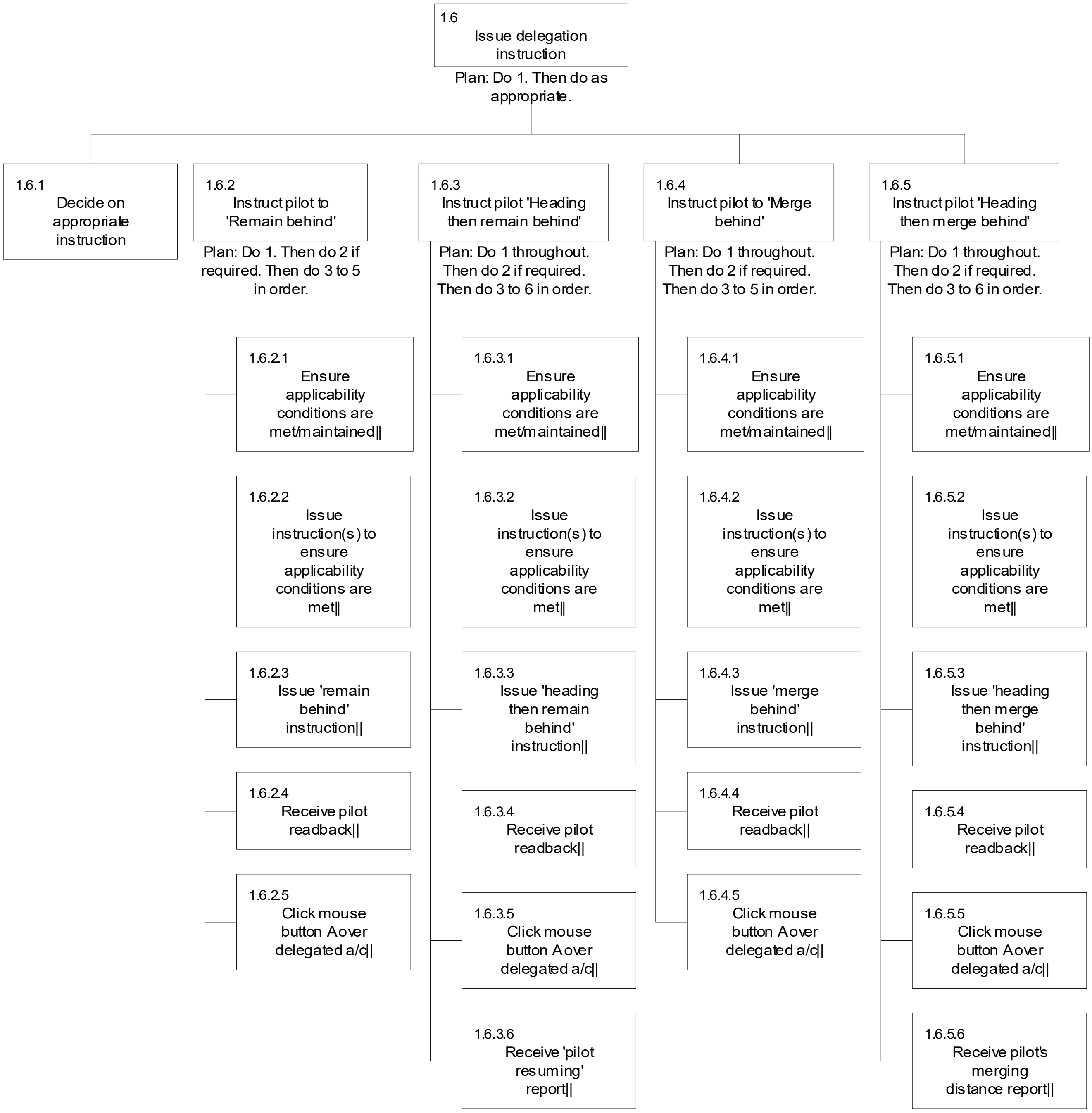
Table 6: Top-level HTA tasks and implications identified for Co-space

HTA Top Level Tasks	Implications identified for Co-space?
1. Conduct task of Extended TMA Controller using Co-space	
Plan: Do 1.1 at start of shift. Do 1.2, 1.3 and 1.4 as appropriate. For delegation aircraft do 1.5, 1.6 and 1.7 in order. Do 1.8 near sector boundary. Do 1.9 at end of shift.	
1.1 Take over from off-going controller	Yes
1.2 Receive aircraft	Yes
1.3 Maintain traffic separation within sector	Yes
1.4 Form sequence plan / Follow sequence formed by AMAN	Yes
1.5 Conduct identification Phase	Yes
1.6 Issue delegation instruction	Yes
1.7 End delegation	Yes
1.8 Transfer to next sector	Yes
1.9 Handover control to relief controller	Yes

All nine tasks were thought to have implications for Co-space. Tasks 1.5, 1.6 and 1.7 were largely new tasks, while other tasks exist currently in a very similar form, with some modifications or different implications for Co-space. An extract of the HTA for Task 1.6 ‘Issue Delegation Instruction’ is shown in Figure 4.

The TRACEr-lite analysis was therefore conducted on the HTA. The categories used for analysis in the TRACEr-lite analysis tables were those presented in Table 6.

Figure 4: Extract of Co-space HTA for Task 1.6 'Issue Delegation Instruction'.



4.3 Comparison of Results

Providing a general comparison of the findings generated by the two approaches presents some difficulties, which need to be borne in mind, as follows:

- TRACEr-lite analysed more tasks than HAZOP. Of the top-level HTA tasks shown in Table 4, HAZOP considered only ‘Task 1.5 Conduct Identification Phase’ and part of Task 1.6 Issue delegation instruction’ (‘Task 1.6.4 Instruct pilot to merge behind’). This was because HAZOP is time- and resource-intensive, and only a one-day meeting was possible.
- The HAZOP and TRACEr-lite studies analysed errors at different levels. TRACEr-lite analysed errors at a more detailed level, but did not take into account simple combinations of events and some external influences, which can be considered to some extent with HAZOP.
- HAZOP considered both pilot and controller errors, as well as a limited number of equipment-related issues. TRACEr-lite considered only controller errors. This was because the HTA only concentrated on controller tasks.

Since HAZOP analysed fewer tasks, it is only possible to compare HAZOP and TRACEr-lite findings for those tasks analysed by HAZOP (Tasks 1.5 and 1.6 in Table 6).

4.3.1 Errors and Issues

The full HAZOP session worksheets and recommendations are included in the Annex report (Appendix A.9). The total pool of errors identified by HAZOP is shown in Table 7 below. For Phase 1, HAZOP identified 26 errors and issues relating to controller error, pilot error or other issues, such as information display. For Phase 2, 29 errors and issues were identified. However only a small number of these had significant consequences in terms of potential for loss of separation or aircraft collision.

The detailed TRACEr-lite analysis for controller tasks related to the implementation of Co-space is presented in the Annex report (Appendix A.10). For Phase 1 (Task 1.5: ‘Conduction Identification Phase’), TRACEr-lite identified around 31 ‘unique’ errors (some of these errors were repeated for different subtasks). For Phase 2, (Task 1.6 ‘Issue delegation instruction’), TRACEr-lite identified 22 ‘unique’ errors (again, some repeated with subtle variations for different delegation scenarios).

Tables 7 and 8 provide a comparison of the errors and issues identified by HAZOP and TRACEr-lite (jointly and separately).

<u>Table 7:</u> Errors and issues identified by HAZOP and TRACEr-lite for Task 1.5 ‘Conduct Identification Phase’.

Error/Issue	In-scope HAZOP?	In-scope TRACEr-lite?
Issues identified by both TRACEr-lite and HAZOP		
Controller instructs pilot to select wrong target	Yes	Yes
Controller goes straight to delegation without confirmation from pilot (fails to detect / query missing readback or target identification)	Yes	Yes
Controller goes straight to instruction of delegation omitting to identify target	Yes	Yes
Controller issues correct target selection instruction to wrong aircraft	Yes	Yes
Controller gives wrong target to correct aircraft	Yes	Yes
Controller gives wrong information to wrong aircraft	Yes	Yes
Controller undertaking another task while giving delegation instruction to a pilot	Yes	Yes
Controller issues unclear instruction – pilot not sure what to do	Yes	Yes
Shift change	Yes	Yes
Issues identified by HAZOP only		
Controller may give other instruction along with delegation instruction	Yes	Yes
Pilot doesn't confirm he has heard the target *	Yes	No
Pilot doesn't read back the target reference *	Yes	No
Pilot selects wrong target	Yes	No
Pilot identifies correct target and goes straight to next action because he feels threatened **	Yes	No
Pilot identifies correct target and anticipates controllers instruction **	Yes	No
Pilot carries out an action before delegation occurs e.g. slows down **	Yes	No
Pilot requests more information	Yes	No
No action taken by pilot or pilot takes too much time to identify target. *	Yes	No
Plot undertaking other task while undertaking delegation	Yes	No
Unclear instructions (equipment)	Yes	No
Pilot and controller receiving different (visual) information	Yes	No
Pilot experiencing difficulties in cockpit	Yes	No
Emergency (pilot or controller)	Yes	No
Severe weather (could be cause of rejection)	Yes	No
Additional training in use of delegation required for pilots	Yes	No
Additional training in use of delegation required for controllers	Yes	No
Issues identified by TRACEr-lite only		
Controller fails to instruct pilot to position target	Yes	Yes
Controller issues wrong / inappropriate instruction	Yes	Yes
Controller fails to detect / query erroneous readback	Yes	Yes
Controller fails to select aircraft on radar	Yes	Yes
Controller clicks wrong mouse button when selecting aircraft on radar	Yes	Yes
Controller selects target aircraft instead of delegated aircraft when selecting on radar	Yes	Yes
Controller selects delegated aircraft instead of target aircraft when selecting on radar	Yes	Yes
Controller selects unintended aircraft (not part of delegation) when selecting on radar	Yes	Yes
Controller fails to detect / query failure to position	Yes	Yes
Controller fails to query spurious position	Yes	Yes
Controller fails to detect / query mis-identification	Yes	Yes
Controller fails to detect / query pilot rejection	Yes	Yes
Controller fails to issue instruction to cancel target	Yes	Yes
Controller issues cancellation instruction to wrong aircraft	Yes	Yes
Controller issues unclear cancellation instruction	Yes	Yes
Controller fails to detect / query failure to deselect	Yes	Yes

Error/Issue	In-scope HAZOP?	In-scope TRACEr-lite?
Controller fails to detect / query non-response to cancellation instruction	Yes	Yes
Controller fails to query spurious response to cancellation instruction	Yes	Yes
Controller fails to deselect aircraft	Yes	Yes
Controller clicks wrong mouse button when deselecting	Yes	Yes
Controller deselects target aircraft instead of delegated aircraft	Yes	Yes
Controller deselects unintended aircraft not part of focused delegation	Yes	Yes

* Failure(s) of associated ATCO hearback identified

** Failure(s) of associated ATCO monitoring identified

For Task 1.5 'Conduct Identification Phase', Table 7 shows that eight errors were identified by both HAZOP and TRACEr-lite.

HAZOP identified eighteen ATCO errors that were not identified by TRACEr-lite, though seventeen of these were outside the scope of the TRACEr-lite analysis (i.e. pilot errors, equipment or information problems or performance conditions / situational factors). For eight of the 18 eighteen issues identified only by HAZOP, TRACEr-lite identified failures in the ATCO response, or identified associated errors.

TRACEr-lite identified twenty-two ATCO errors that were not identified by HAZOP, associated with controller-pilot communications and controller-interface interactions.

Table 8: Errors and issues identified by HAZOP and TRACEr-lite for '1.6.4 Instruct pilot to merge behind' (part of Task 1.6 'Issue delegation instruction')

Error/Issue	In-scope HAZOP?	In-scope TRACEr-lite?
Issues identified by both HAZOP and TRACEr-lite		
Controller fails to notice that applicability conditions are not met/maintained)***	Yes	Yes
Predicted separation at merging point lower than desired separation ***	Yes	Yes
Controller omits to give delegation but thinks s/he have given delegation	Yes	Yes
Controller gives delegations to too many aircraft ***	Yes	Yes
Controller gives inappropriate, unsuitable or incompatible delegation instruction	Yes	Yes
Controller issues wrong delegation instruction (e.g. remain instead of merge instruction)	Yes	Yes
Controller only gives part of instruction (e.g. omits distance or way point) or issues delegation instruction incorrectly	Yes	Yes
Controller loses track of what delegation has been given to which aircraft ***	Yes	Yes
Controller takes too long to give delegation instruction after giving target	Yes	Yes
Controller undertaking another task while giving delegation instruction to a pilot ***	Yes	Yes
Controller issues unclear instructions (not clear to pilot what s/he is supposed to do)	Yes	Yes
Issues identified by HAZOP only		
Controller gives superfluous instructions	Yes	Yes
Aircraft not flying straight to merging point **	Yes	No
After merging point aircraft not flying on same trajectory **	Yes	No
Pilot does not adjust speed **	Yes	No
Pilot reduces speed too much **	Yes	No

Error/Issue	In-scope HAZOP?	In-scope TRACEr-lite?
Pilot increases speed too much **	Yes	No
Controller gives correct instruction but pilot takes wrong action (other than delegated instruction) *	Yes	No
Pilot takes additional action not requested by controller **	Yes	No
Pilot takes too long to take action (time constraints given by way point - spacing) **	Yes	No
Pilot receives more information on cockpit display	Yes	No
Pilot gives more information to controller than required.	Yes	No
Pilot undertaking other task while undertaking delegation	Yes	No
Unclear instructions (equipment)	Yes	No
Pilot and controller receiving different (visual) information	Yes	No
Issues identified by TRACEr-lite only		
Controller fails to issue instruction to ensure applicability conditions are met/maintained	Yes	Yes
Controller issues wrong or unsuitable instruction to ensure applicability conditions are met/maintained	Yes	Yes
Controller issues instruction to ensure applicability conditions are met/maintained to wrong aircraft	Yes	Yes
Controller issues delegation instruction to wrong aircraft	Yes	Yes
Controller issues delegation instruction with inappropriate parameter/value	Yes	Yes
Controller fails to detect / query erroneous readback	Yes	Yes
Controller fails to detect / query missing readback	Yes	Yes
Controller fails to select aircraft on radar to indicate 'delegated'	Yes	Yes
Controller clicks wrong mouse button when indicating 'delegated' on radar	Yes	Yes
Controller selects target aircraft instead of delegated aircraft when indicating 'delegated' on radar	Yes	Yes
Controller selects unintended aircraft (not part of delegation) when indicating 'delegated' on radar	Yes	Yes

* Failure(s) of associated ATCO hearback identified

** Failure(s) of associated ATCO monitoring identified

*** Related/similar errors identified

For Task 1.6.4 'Instruct pilot to merge behind (part of Task 1.6 'Issue delegation instruction'), eleven errors were identified by both HAZOP and TRACEr-lite.

HAZOP identified fourteen errors that were not identified by TRACEr-lite, though thirteen of these were outside the scope of the TRACEr-lite analysis. For eight of the issues identified by HAZOP only, TRACEr-lite identified failures in the ATCO response, or identified associated errors.

TRACEr-lite identified eleven ATCO errors that were not identified by HAZOP, again associated with controller-pilot communications and controller HMI interactions.

Additionally, TRACEr-lite examined other scenarios that comprise Task 1.6 'Issue delegation instruction' (i.e. 'Instruct pilot to remain behind', 'Instruct pilot heading then remain behind', 'Instruct pilot heading then merge behind'). Most of the errors shown in Table 8 above are repeated for these scenarios, but some new errors also appear.

TRACEr-lite also analysed another seven high-level tasks that were not analysed in the HAZOP session (see Table 6). The errors identified by TRACEr-lite for these tasks are not included in this comparison, but can be seen in the Annex report, Appendix A.11. The main tasks affected by Co-space in terms of errors predicted were:

- 1.3 Maintain traffic separation within sector
- 1.4 Form sequence plan / Follow sequence formed by AMAN
- 1.5 Conduct Identification Phase
- 1.6 Issue delegation instruction
- 1.7 End delegation

When considering all nine tasks and each associated detailed subtask, the total number of detailed errors predicted totalled around 280. However, many of these were basically the same errors repeated for different subtasks (e.g. failures in reviewing flight progress strips, receiving pilot RT readbacks, or indicating delegation status on radar). When considering different errors for each of the top-level tasks, the number reduces to around 160 errors. Of these, 78 errors were rated as moderate Recovery Success Likelihood (RSL), 17 were rated as low-moderate RSL, and one was rated as low RSL. The remaining errors were rated as either high or moderate-high RSL[10].

4.3.2 Possible Consequences

The HAZOP study found the following possible consequences for the phases/tasks above.

- Controller may pay too much attention to particular aircraft.
- Delegation task may take precedence over normal flying action (endanger flight).
- Pilot delay in undertaking controller's instruction.
- Pilot can't implement instruction or omits to comply with instructions.
- Pilot doesn't select target/undertake action.
- Pilot executes given incompatible instruction.
- Multiple speed adjustments by pilot and for trailing arrival stream.
- Knock on problems during sector transfer.
- Trailing traffic sequence may be impacted.
- Frequency occupancy.
- Increase in workload for controller and/or pilot.
- Incorrect controller situational awareness.

[10] As noted in the executive summary, this apparent level of error should not be taken out of context, since the study has only focused on negative aspects and has not considered safety advantages of the three projects.

- Infringement of separation/spacing.

The TRACEr-lite analysis showed that for Task 1.5 Conduct Identification Phase, the errors with moderate or low-moderate RSL (none were rated as low RSL) could result in the following summarised consequences:

- Pilot selects/identifies wrong target; controller unaware of failed or non-identification.
- Controller forgets about delegation.
- Pilot fails to select target.
- Controller unaware of pilot rejection; Controller assumes pilot has identified target.
- Applicability conditions not met (aircraft have incompatible performances or speeds, inappropriate trajectories or separations).
- Controller forgets target/delegated aircraft status; Failure to transfer information at handover.
- Pilot does not deselect target.
- Controller forgets aircraft is no longer delegated.
- Pilot and controller have different knowledge states; pilot believes aircraft is under delegation.
- Pilot takes no action; controller falsely believes pilot under delegation.
- Controller forgets or misrecalls delegation or delegation instruction; failure to transfer information at handover.
- Possible loss of spacing or separation.

It is important to note that in the HAZOP and TRACEr-lite methods, consequences are stated irrespective of safeguards, i.e. as if the safeguards did not exist. Safeguards are then identified that could prevent or mitigate the consequences. This process helps to establish the dependency on safeguards, and whether new safeguards are required. Several such safeguards were identified for Co-space, as detailed below.

4.3.3 Safeguards

The safeguards identified by HAZOP were:

- Anti-Overlap software tool on radar display.
- Confirmation of target.
- Controller training and procedural controls.
- Controller finishes targeting before hand over.
- Current pilot support tools in cockpit, e.g. alert or autopilot.

- Marking functions on controller interface allows delegation to be marked for each aircraft.
- Normal flying tasks take precedence over target selection.
- Pilot readback of target, pilot query, pilot refusal of delegation.
- Radar monitoring.
- Target positioning by pilot.
- STCA.
- TCAS.

The safeguards identified by TRACEr-lite were:

- Check on strip markings
- Radar monitoring
- RT communication, Pilot readback, pilot query
- STCA

4.3.4 Co-space recommendations

4.3.4.1 HAZOP-generated recommendations

A number of recommendations were proposed during the HAZOP, as follows:

1. Anti Overlap (display decluttering) as it currently exists needs some improvement. Review how this software tool can be used to support the controller during delegation and what improvements are required for it to be effective.

2. Consider making target positioning by pilot a compulsory subtask in target selection.

3. Explore how data link technology could be used to support both controller and pilot when selecting a target during delegation.

4. Review safeguards for preventing the pilot from acting own initiative to ensure that they are adequate.

5. Assess performance limits of delegation in terms of maximum number of delegations that can be managed by the controller and impact of abnormal conditions such as response to errors or delay.

8. Implement a suitable training programme for both pilots and controllers in the application and use of delegation.

9. Ensure controller and pilot procedures are easily understood and adequately support delegation requirements.

10. Review and identify available controller monitoring assistance tools to support early detection or prevent occurrence of separation infringement.

11. Provide more information and guidance on how display marking for the data link and delegation instruction is to be used.

12. Review how the existing marking functions on the controller interface can be used to support the controller during delegation and what improvements are required for it to be effective.

13. Review how data link technology can be used to automatically confirm pilot action (mode activation) prior to changes being seen on controller's radar.

14. Review how existing and potential safeguards and supporting tools for pilot and controller can be used to prevent errors rather than respond to them.

15. Controller training should include guidance on what information needs to be given at specific times during delegation.

16. Review how data link technology could be used to support pilot during delegation and what improvements are required for it to be effective.

4.3.4.2 TRACEr-lite-generated recommendations

A number of recommendations were generated by TRACEr-lite that may help to resolve individual errors. These were as follows:

1. Controllers should have a handover protocol to ensure that all critical information relation to delegated aircraft in transferred correctly.
2. Controllers should have a permanent (electronic or written) indication of delegation status, type of application and associated parameters.
3. Any indication of delegation status, type of application and associated parameters should be present also for transferred aircraft.
4. It is important that the controller marks aircraft as delegated on Radar Display at all times.
5. The controller will in future have many items to check on the flight plan/strip or other media (in addition to ASAS equipage). Hence, an analysis of critical items should be performed.
6. Conditions for the cancellation of delegation in maintaining traffic separation assurance should be clarified in procedures and training.
7. The importance of checking applicability conditions are (still) met should be emphasised periodically in training.
8. The pilot should position the target to avoid errors in target selection.
9. Progress of delegation should be supported by automatic compliance monitoring if possible.
10. An aide memoire may be necessary initially to help the controller to check all applicability conditions.
11. It should be ensured that the pilot can only select the target intended by the controller.
12. Controllers should be trained to ensure HMI operations related to selection/delegation are completed simultaneously with RT communication

(or immediately after any required strip marking performed simultaneously with RT communication).

13. Consider incorporating a controller readback for pilot resuming reports and reports of merging distance.
14. Consider incorporating a controller readback for pilot notification to unable delegation.

4.3.5 Discussion of the Application of HAZOP and TRACEr-lite to Co-space

Overall, HAZOP and TRACEr-lite identified a similar number of errors and issues for the two tasks analysed. However, HAZOP included both controller and pilot errors, as well as a small number of other issues. TRACEr-lite focussed solely on controller errors. Hence, for controller errors, TRACEr-lite was more comprehensive and detailed in error prediction; HAZOP did not identify over 60% of the total number of controller errors identified in the study. It may be, however, that some of these errors would be predicted by HAZOP given more time to consider the two tasks.

HAZOP identified a similar range of possible consequences to TRACEr-lite, though the TRACEr-lite consequences tended to be limited to the more immediate, short-term consequences. HAZOP, however, identified significantly more safeguards than TRACEr-lite. One area of concern however, was the dependency on developing technology able to support the controller and pilot. Two critical issues related to this are the timing of implementation (e.g. data-link technology), and the independence of other projects (i.e. outside the scope of control of the Co-space project).

The Recovery Success Likelihood rating used by TRACEr-lite was useful in filtering the errors predicted, and the ratings were moderated by members of the Co-Space team to help ensure that they were realistic. Only around 12% of the total number of RSL ratings for all errors predicted for all nine tasks were changed, thus suggesting that the initial RSL ratings were reasonably realistic. The RSL concept may be useful to consider incorporating into the HAZOP method. It would also be useful to rate error likelihood within a TRACEr-lite analysis. This was not within the scope of this study, but could be performed in future using expert judgement (see Kirwan, 1994), potentially with a simple scale – possibly anchored - from ‘low’ to ‘high’.

The project team found the HAZOP risk matrix (see Appendix A.9) difficult to apply to the majority of the errors identified. This is a common issue in ATM, where severity and likelihood analysis is much more difficult than in other issues, largely due to the highly dynamic nature of ATM.

HAZOP and TRACEr-lite generated a similar number of recommendations, but the TRACEr-lite recommendations related to all nine tasks. Hence, HAZOP is clearly more productive in identifying recommendations. It would be useful in future TRACEr-lite analysis to involve the project team in the generation of recommendations.

5. DISCUSSION

5.1 General Overview of the Study

This study applied the Human Error Analysis techniques TRACEr-lite and HAZOP to three EUROCONTROL projects: Co-space, Time-Based Separation and CORA 2. It was not an objective of the study to perform a safety assessment, but rather to provide an illustration of the potential analyses that could be performed, and their added value to design and safety. The results from all three applications were broadly similar. In general, a detailed range of errors and issues were predicted by the techniques. HAZOP addressed controller and pilot issues, as well as some information and equipment issues. TRACEr-lite identified most of the controller errors identified by HAZOP, but focussed more deeply on controller errors and was more comprehensive in identifying these. Both techniques identified a range of possible consequences and safeguards, though HAZOP took better account of the operational context. A number of recommendations were generated by the techniques, and again HAZOP was more productive in this respect because if the involvement of the project teams. However, TRACEr-lite was the more resource efficient of the techniques.

Overall, both HAZOP and TRACEr-lite proved useful methods to support designing for safety, and integrated well with the projects. For the CORA 2 project, the HAZOP was less useful than for the other projects, because a similar analysis had previously been performed as part of a safety assessment. Similarly, the TBS project was in a very early stage of concept development, and so the TRACEr-lite analysis was somewhat premature in trying to predict errors in detail, but the associated task analysis helped to identify further issues for the project to address. The use of HAZOP in this study focused primarily on human and information-related issues, since these were the core issues affecting the projects at this stage and it was not possible to perform a detailed HAZOP for hardware and software. However, the HAZOP approach can be used to perform such analyses when the projects are at the appropriate stage.

It would be useful to use a hybrid approach by performing a preliminary HAZOP to identify the core tasks and critical, high-level errors followed by a detailed TRACEr-lite analysis. This HAZOP could also identify the relevant safeguards and consequences for use in the detailed TRACEr-lite analysis, to improve the contextual relevance of the technique. HAZOP can also be modified to assess Human-Machine Interfaces (e.g. Kennedy, *et al*., 2000) when interface design mock-ups are available. HAZOP and TRACEr-lite represent two useful techniques that could be used as part of a portfolio of methods (Shorrock, *et al*., 20001b) available to support ‘design for safety’. Section 5.2 analyses the relative performance of the techniques in more depth, and section 5.3 gives practical, high-level guidance for using these two techniques for ATM applications.

5.2 Detailed Discussion of Techniques

In order to facilitate the discussion and comparison of HAZOP and TRACEr-lite as applied to EUROCONTROL projects, the following criteria for the evaluation of human error analysis methods are used:

- Comprehensiveness - the ability to discriminate and classify a comprehensive range of errors and influencing factors.
- Life cycle applicability - the degree to which the technique can be used throughout the formative and summative (later) phases of system design lifecycle.
- Theoretical validity - whether the technique is based on a model of human performance, with a theoretically plausible internal structure.
- Operational validity (realism) - the degree to which the technique adequately captures contextual information.
- Flexibility - whether the technique enables different levels of analysis according to the project needs, known information or expertise of the user.
- Usefulness - whether the technique suggests, or can generate, error reduction or mitigation measures.
- Resource efficiency (training) - the time taken to become proficient in the use of the technique.
- Resource efficiency (usage) - the amount of time required to collect supporting information and conduct the analysis.
- Usability - the ease of use of the technique.
- Auditability - the degree to which the degree lends itself to auditable documentation.

Unfortunately, it was not within the scope of the project to evaluate:

- Consistency - the degree to which the technique leads to consistent analyses between different users and with the same user over time.
- Predictive accuracy - the degree to which the technique accurately predicts potential errors that occur subsequently (e.g. in simulation).

5.2.1 Comprehensiveness

HAZOP and TRACEr-lite performed differently on the issue of comprehensiveness. HAZOP identified both controller and pilot errors while considering each task, and also examined potential information and equipment problems. However, in the time available, HAZOP could only examine two tasks for Co-space, and one task for TBS and CORA 2. TRACEr-lite examined a wide range of controller tasks for each project, and provided a highly comprehensive and detailed ‘register’ of potential errors. However, TRACEr-lite examined only controller errors (because controller tasks were the focus of the HTA).

TRACEr-lite tended to analyse the errors ‘flagged’ by HAZOP in a more detailed and systematic fashion. This is largely because TRACEr-lite uses a detailed HTA, while HAZOP is often not conducted at this fine level of task modelling. However, one of the potential dangers of detailed TRACEr-lite analysis is in getting ‘lost in detail’ and failing to identify more fundamental issues. While this did not seem to occur in the current analysis, it is a potential problem to be aware of. However, to complete the HAZOP and to provide a fairer comparison, a further set of sessions would have to be held for the remaining tasks not analysed by HAZOP.

The analysis showed that TRACEr-lite identified approximately 91% of the errors/issues identified by HAZOP that were within the scope of the TRACEr-lite analysis (i.e. controller errors). For issues and errors identified by HAZOP that were outside the scope of the TRACEr-lite analysis (such as pilot errors and general performance conditions), TRACEr-lite was able to predict related errors, such as failures in ATCO responses to pilot errors for approximately 36% of the issues.

HAZOP identified approximately 42% of the errors identified by TRACEr-lite for Co-space, TBS and CORA 2[11] However, as previously stated, HAZOP identified other issues such as pilot errors and controller performance conditions that were not analysed by TRACEr-lite. On the basis of this comparison, it could be concluded that TRACEr-lite is more comprehensive in identifying detailed errors, more systematically, but HAZOP may better capture the ‘big picture’ and focus on the most important areas.

5.2.2 Life cycle applicability

Both HAZOP and TRACEr-lite demonstrated that they could be used throughout the formative and summative phases of system design lifecycle. TBS was in an early conceptual stage, while CORA 2 was in the design stages, and Co-space was in the simulation phases. However, TRACEr-lite’s need for a more detailed task analysis would prompt the conclusion that HAZOP is more suited to projects in the conceptual and pre-design stages of development. A useful approach would be to conduct a preliminary HAZOP initially, to focus the analysis, identify the primary sub-tasks of interest, and identify the fundamental errors, then follow this up with a detailed TRACEr-lite analysis to help ensure that errors are captured at a detailed and comprehensive level.

5.2.3 Theoretical validity

TRACEr-lite is based on a model of human performance, with a theoretically plausible internal structure. While HAZOP does not have this foundation, the guidewords are developed from theoretically valid human performance outcomes.

[11] It is difficult to give precise statistics due to differences in the level of granularity of identified errors. This figure is based on the figures presented in Section 6 (i.e. very detailed TRACEr-predicted errors are not included or are combined).

5.2.4 Operational validity (realism)

HAZOP and TRACEr-lite account for context in different ways. HAZOP primarily uses the expertise of the HAZOP team. This is an established method of ensuring that such analyses are contextually relevant. TRACEr-lite uses project personnel and documentation to construct and review the Context Statement and Task Analysis. The project personnel would also then review the TRACEr-lite analysis. This is an important post-analysis step, which would involve face-to-face discussions between the TRACEr-lite analyst and project personnel, perhaps also considering error likelihood and severity, but was not possible during this study due to time and resource constraints[12]. Some of the TRACEr-lite predicted errors may, therefore, appear somewhat 'naïve'. However, equally, there are positive arguments in favour of this. Project team members who are very 'close' to the project' may consider certain errors 'incredible' in a HAZOP analysis, and prefer not to propose or record them. From a TRACEr-lite point of view, on the other hand, such errors would be logical possibilities. Overall during this study, considering the errors and issues predicted, consequences, safeguards and recommendations, HAZOP outperforms TRACEr-lite on this criterion.

5.2.5 Flexibility

Both HAZOP and TRACEr-lite are flexible in that they allow different levels of detail in the analysis. HAZOP has the advantage that early in the concept development/selection process, a preliminary HAZOP can be performed, using the creative brainstorming and knowledge of the group. The full HAZOP technique can then be performed later. TRACEr-lite, however, requires a more developed task analysis, since the individual analyst is not qualified to perform such a 'brainstorming' approach. TRACEr-lite does, however, provide flexibility in the use of Internal Error Modes and Mechanisms – the use of Mechanisms in the analysis can be omitted or used only for critical errors. TRACEr-lite can also be used in a small group-based format, using the Error Domains Perception, Memory, Decision, and Action as prompts. Indeed, this method has previously been incorporated into the Human HAZOP method to better account for cognitive aspects of errors in other HAZOP studies.

5.2.6 Usefulness

Both HAZOP and TRACEr-lite helped to produce error reduction or mitigation measures. The HAZOP analysis produced more traditional recommendations while TRACEr-lite tended to produce 'performance requirements', which could be fulfilled in a number of ways. The HAZOP method, however, was clearly much more productive in this respect, owing to the contribution of the project teams. The project team could, in future, participate similarly in generating recommendations based on TRACEr-lite findings.

[12] The TRACEr-lite synthesis was reviewed by the Co-Space project team.

5.2.7 Resource efficiency (training)

This criterion has not been formally tested, but training to become a HAZOP facilitator would normally involve three to four days training, and prior experience as a recorder. No training is required to act as a participant but awareness or familiarisation training is very useful to speed up the process. HAZOP's training requirement is largely associated with the ability to facilitate a group-based process. The role of the HAZOP leader or TRACEr-lite analyst may not suit every individual, and the HAZOP leader role requires different skills to the TRACEr-lite analyst role. Training in the use of the TRACEr-lite technique would normally involve 1-2 days, plus a further 1-2 days to learn how to use Hierarchical Task Analysis. Hence, the training demand for each technique is quite similar.

5.2.8 Resource efficiency (usage)

The HAZOP and TRACEr-lite studies are compared on the resource efficiency (usage) criterion below in Table 9. This compares the two techniques for an equivalent analysis. Hence, these estimated figures reflect a full analysis for all controller high-level tasks in the CORA HTA.

Table 9: Resource requirements for HAZOP and TRACEr-lite for an equivalent analysis.

Tasks	**Person days required per project for equivalent analysis**	
	HAZOP	**TRACEr-lite**
Background familiarisation	1	1
Task Modelling	1	3
Review	0.5 (0.25 day x 2 people)	0.5 (0.25 day x 2 people)
Analysis	18 (3 days x 6 people)	4
Data formatting tidying, etc.	1	0.5
Review	1 (0.25 x 4 people)	1 (0.5 day x 2 people)
Revise	0.5	1
Reporting	2	3
Review	1 (0.5 x 2 people)	1 (0.5 day x 2 people)
Revise	0.5	1
Total person-days	**26.5**	**16**

This comparison suggests that TRACEr-lite is the more resource efficient technique.

5.2.9 Usability

Both HAZOP and TRACEr-lite are usable techniques. HAZOP has stood the test of time, and does not demand complex analysis from participants. However, the process can prove tiring, particularly where several unbroken days of analysis are performed. In this respect, it is wise to break up sessions that occur over several days (though care should be taken to ensure that a ‘flow’ is maintained in the study). TRACEr-lite, similarly, can be frustrating to the analyst due to the repetitive nature of analysis.

The HAZOP process was, on the whole, received positively by those who participated in the sessions. The project teams reported benefits in taking a high level overview and gained value from the process of identifying and prioritising human error issues by the potential consequences.

5.2.10 Auditability

Again, both HAZOP and TRACEr-lite provided a fully auditable process, with worksheets demonstrating the reasoning behind the analysis. HAZOP, additionally, visually projected each worksheet during the session so that all of the participants could verify the findings ‘on-line’.

5.3 Recommendations for the Use of the Techniques in Further ATM Projects

The application of procedural HAZOP to Co-space, TBS and CORA 2 produced the following recommendations for the future use of HAZOP and TRACEr-lite by EUROCONTROL:

The application of these two techniques to Co-space, TBS and CORA 2 produced the following recommendations for the future use of HAZOP and TRACEr-lite by EUROCONTROL:

1. For projects without detailed procedures or task descriptions, the preliminary HAZOP methodology is most appropriate for use by EUROCONTROL. This should identify the core tasks and critical, high-level errors, as well as the relevant safeguards and consequences. A detailed TRACEr-lite analysis should be conducted after the preliminary HAZOP, making use of the information derived from the HAZOP. For other projects with detailed task and system descriptions, the full HAZOP method may be used.

2. The HAZOP method can be modified to be used to assess Human-Machine Interfaces (e.g. Kennedy, et al., 2000). This variation of the HAZOP approach would probably reflect more closely a TRACEr-lite analysis, and could be explored by project teams when interface design options are available.

3. In future sessions, there should always be a human factors specialist, safety specialist and a controller / pilot as a user representative on the HAZOP team.

4. A trained and experienced HAZOP leader should always lead the HAZOP session. It would also be beneficial where project teams have not used HAZOP before to have a short training session prior to commencing the project.

5. Full HAZOP sessions should be no shorter than 2 days, and normally 3-5 days. Preliminary HAZOPs for scoping purposes may be performed over one day in order to provide a high-level *identification* of the potential errors associated with a project.

6. One area of concern is the identification and implementation of appropriate safeguards or recommendations. Safeguards must be currently available or formally planned. Due to the integrated nature of EUROCONTROL projects, reliance is often placed on processes and technology that are also under development but outside the scope of the project. Care needs to be taken that lessons learned from one project are shared and/or incorporated into other projects and that the documented safeguards and recommendations are carried through to the operational phase of the project where appropriate.

7. Hierarchical Task Analysis should be performed using an easy-to-use, automatic hierarchical drawing package, able to export the associated text to Rich Text Format.

8. The use of TRACEr-lite's Internal Error Mechanisms is not necessary for the general TRACEr-lite analysis since the value of using error mechanisms is not justified by the analytical effort. However, they may be useful after the general analysis to examine the psychological causes of errors that are of high frequency, high severity, or low Recovery Success Likelihood (RSL).

9. Human error likelihood and criticality should be rated in future TRACEr-lite analyses in conjunction with the project teams, including operational specialists. The suitability of any risk ranking method needs to be considered carefully before us in HAZOPs.

10. The output of the error analysis should be reviewed by members of the project team including operational specialists, prior to formulation of recommendations and write-up.

6. CONCLUSIONS

The following conclusions have emanated from the study:

- Overall, both HAZOP and TRACEr-lite proved useful methods to support designing for safety. Both techniques were successful in identifying errors and issues, their associated consequences and safeguards, and recommendations for further action.
- HAZOP and TRACEr-lite have a slightly different focus. HAZOP tended to operate at a higher level of analysis, while TRACEr-lite focused on tasks and associated actions in more detail.
- HAZOP is more resource intensive than TRACEr, analysing fewer tasks in a similar number of person-days.
- HAZOP and TRACEr-lite could be best employed together as a hybrid approach. Each technique has different advantages and disadvantages, and so each technique compensates for the other's weaknesses.
- HAZOP and TRACEr-lite are ready to be applied to further EUROCONTROL projects. Such applications, in a safety case context, would need more complete assessments, also considering the potential safety benefits of the concepts being evaluated.

7. REFERENCES

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

EATMP (2002). *CORA 2 Operational Concept of Use*. ASA.01.CORA.2.DEL01.OCU, V1.0, Proposed Issue.

EATMP (2002). *CORA 2 HMI document*. V0.1, Draft.

EATMP (2002). *Model of the Controller-CORA 2 Interaction. The controller's task of conflict resolution in a CORA 2 environment*. Working Draft.

EATMP (2002). *Operational Scenario Document*. ASA.01.CORA.2.DEL05-B.OSD, V0.3, Draft.

Embrey, D.E. (1986) SHERPA: A systematic human error reduction and prediction approach. *Paper presented at the International Topical Meeting on Advances in Human Factors in Nuclear Power System*s, Knoxville, Tennessee.

EUROCONTROL (2001). *Freer Flight: Evolutionary Air-Ground Co-operative ATM Concepts (EACAC). Procedures of Delegation of Separation from the Controller to the Flight Crew*. Version 2.2. Issued 13 November 2001. (This contained procedures and RT protocol.)

EUROCONTROL (2002). *CoSpace Real-Time Experiment Briefing Document*. Version 1.1. Issued 07 November 2002. (This contained delegation interface diagrams.)

Isaac, A., Shorrock, S.T. and Kirwan, B. (2002). Human error in European air traffic management: the HERA Project. *Reliability Engineering and System Safety*, **75 (2)**, 257-272.

Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method: CREAM*. Oxford, UK: Elsevier.

Kennedy, R., Jones, H., Shorrock, S. and Kirwan, B. (2000). A HAZOP analysis of a future ATM system. In P.T. McCabe, M.A. Hanson and S.A. Robertson, *Contemporary Ergonomics 2000*. London: Taylor and Francis.

Kirwan, B. (1994). *A Practical Guide To Human Reliability Assessment*. London: Taylor and Francis.

Kletz, T.A. (1988). *What Went Wrong?: Case Histories of Process Plant Disasters*. US: Gulf Publishing.

Kletz, T.A. (1999). *Hazop and Hazan: Identifying and Assessing Process Industry Hazards*. Rugby, UK: IChemE.

Leroux, M. (2000). Cognitive aspects and automation. In N.B. Sarter and R. Amalberti (Eds.), *Cognitive Engineering in the Aviation Domain*. London: Laurence Erlbaum Associates.

Livingston, A. (2001). Team approach to human error assessment. *IBC Seminar on Human Error Techniques*, October 2001, London.

Sarter, N. and Woods, D.D. (1995b). *Strong, Silent, and Out-of-the-Loop: Properties of Advanced (Cockpit) Automation and their impact on Human-Automation Interaction*. Technical Report CSEL 9-TR-01. Columbus, OH: CSEL, Ohio State University.

Shepherd, A. (2001). *Hierarchical Task Analysis.* London: Taylor and Francis.

Shorrock, S.T. (2002a). The two-fold path to human error analysis: TRACEr-lite retrospection and prediction. *Safety Systems* (Newsletter of the Safety-Critical Systems Club), Vol. 11 No. 3, September 2002.

Shorrock, S.T. (2002b). Error classification for safety management: finding the right approach. Proceedings of the *Workshop on the Investigation and Reporting of Incidents and Accidents*, 17th to 20th July 2002, The Senate Room, University of Glasgow.

Shorrock, S.T. and Kirwan, B. (1999). TRACEr: a technique for the retrospective of cognitive errors in ATM. In D. Harris (Ed.) *Engineering Psychology and Cognitive Ergonomics: Volume Three - Transportation Systems, Medical Ergonomics and Training.* Aldershot, UK: Ashgate.

Shorrock, S.T. and Kirwan, B. (2002). The development and application of a human error identification tool for air traffic control. *Applied Ergonomics*, **33**, 319-336.

Shorrock, S.T., Kirwan, B., MacKendrick, H. , Scaife, R. and Foley, S. (2001a). The practical application of error analysis in UK ATM. Proceedings of *People in Control: An International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres*, UMIST, Manchester, UK: 18 - 21 June 2001.

Shorrock, S.T., Kirwan, B., MacKendrick, H. and Kennedy, R. (2001b). Assessing human error in Air Traffic Management systems design: methodological issues. *Le Travail Humain*, **64 (3)**, 269-289.

Wiener, E.L. (1985). Cockpit automation: in need of a philosophy. *Proceedings of the 1985 Behavioural Engineering Conference*, Warrendale, PA, 1985, pp. 369-375.

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

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