N95-34768

Certification of Tactics and Strategies in Aviation

Hartmut Koelman

EUROCONTROL

The Need for Operational Concepts

The author's interest in Operational Concepts stems from his work at Eurocontrol, which is related to Air Traffic Management (ATM). Further details can be found in the annex of this paper (the European need for ATM Operational Concepts). These show that the "tactics and strategies" subject is not just to be seen as an academic research issue, but that there is a need for tangible results in the coming years to support the system innovation efforts which will see operational and industrial application after the year 2000.

But what is meant by the terms "tactics and strategies"? A story can help to clarify this. The author is a system analyst at Eurocontrol, but he is also a flight instructor at the University of Leuven (KU Leuven, Belgium). Although the prime purpose of the latter activity is to teach student pilots how to fly sail planes in flatland and mountain environments, it is also a platform for observing and analyzing human behavior.

As a flight instructor, one observes a variety of student shortcomings: insufficient perception of events, lack of situational awareness, lack of anticipation, inability to keep up with the rapid succession of events, faulty judgements, improper setting of priorities, lack of insight in cause-effect relationships, loss of concentration, etc. One also observes the learning curve in student pilots: from when they master attitude control and think that they can fly (except that the instructor has to tell the student what to see, what to do, and when/where/why/how to do it), and through the successive increase in skill and workload capabilities. Whenever a task is mastered, it becomes an automatism.

Automatism causes a workload reduction and the student is ready to tackle a new aspect of flight management. It ends with the situation where the instructor primarily monitors the judgement of the student (with associated problems of underload and boredom for the instructor). Meanwhile, as the instructor, one must constantly keep track of the student's (changing) performance limitations and decide when the student may be exposed to the expanding range of operating conditions. Last but not least, one must know when to take control of the situation so that the safety of the flight is not compromised but the student still learns from his or her mistakes.

Over the years, student after student completes training, and the instructor starts recognising patterns of cognitive behaviour. The conclusion is: everything can be considered a tactic or a strategy. The student masters the tactics needed to deal with a situation. Subsequently, he/she learns strategies which will control the application of those tactics. After that, super-strategies are needed to control the application of the strategies, and so on. The student learns a hierarchy

Human Factors Certification of Advanced Aviation Technologies
Edited by J. A. Wise, V. D. Hopkin, and D. J. Garland

of techniques (i.e., an Operational Concept), starting from short-term anticipation and simple situation tactics to long-term anticipation and complex situation strategies. Many of these techniques are not written down as formal operational procedures, but have to be mentally acquired through personal experience. Finally, the student may develop into the experienced glider pilot who spends months planning and preparing for a world record attempt, waits years for the day with those unique meteorological conditions that the plan requires, and then executes that plan. Thousands and thousands of strategical and tactical decisions are needed in the ten or fourteen hours it takes to complete the flight.

The point is, (for certification, specification or any other purpose) to separate a system just into its design (the static part) and its operation (the dynamic part) is a far too simplistic view of the world, as is the separation of system operation just into strategies (the static part of operations) and tactics (the dynamic part of operations). The stability-volatility spectrum in system characteristics is usually not a black and white picture. It has many shades of grey. For the sake of the argument, it is unwise to allow oneself to become handicapped by a lack of conceptual richness in the English (or any other language's) vocabulary. It may be the case that the understanding of system operation or human cognitive behaviour (i.e., the task analysis) requires a whole hierarchy of planning techniques, with varying degrees of stability (from very tactical to very strategic and design-like). The same is true for the information which describes designs, strategies, tactics and the situational awareness which is associated with the planning techniques on these different levels. The terms "information" and "data" are typically erroneously used to convey the idea that every piece of information is equally significant (a typical engineering mistake). Information should be categorized in accordance with the different planning layers to preserve the operational significance of the different degrees of volatility of the information.

Typical Operational Concepts

An Operational Concept is a model which describes the dynamics of managing an operation. It is expressed in terms of planning and execution responsibilities, control loops and operational procedures. The operation is described for the composite human-machine system.
Traditionally in a composite human-machine system, the human still carries ultimate responsibility for the satisfactory performance of the composite system. Hence, the planning and execution responsibilities, control loops and operational procedures mentioned in the glider example, although supported by machines (automation), are primarily a human factors concern.

Operational Concept for Air Traffic Management (ATM)

If we look at the way ATM is organised today, and most likely still will be organised in the year 2015, we see the use of planning "layers" with different planning horizons (Eurocontrol, June 1992; EATCHIP Task Force on ATC System Integration, June 1992). The general objective for each layer is to deliver an acceptable situation to the next layer. Each layer works as a "filter" for the following one. This *filtering strategy* defines specific roles for each layer, with the higher layers addressing a general scope and a long planning horizon, and the lower

layers concentrating on specifics and short planning horizons. A typical layering for ATM is as follows.

Development of Operational Concepts, standards and recommended practices on worldwide and regional scale (10 – 15 years lookahead): serves to provide guidance for system procurement actions and aircraft mandatory carriage requirements, items which have lead times of 5 – 10 years typically.

Planning the renewal and upgrade of infrastructure on regional and sub regional scale (5 – 10 years lookahead): deals with site construction, development and procurement of hardware/software, and strategic human resource planning.

Strategic Airspace Management (ASM) on a regional scale (several years lookahead): defines basic strategies for ATS Route Networks (ARN), airspace use (segregation/flexible), and traffic segregation.

Strategic Air Traffic Flow Management (ATFM) on regional scale (up to one year lookahead): strategic ATFM activities are intended to resolve major demand/capacity imbalance problems and generally concern summer traffic flow. They result in a Traffic Orientation Scheme based on published flight schedules, airspace structure and system structure and capacity. After processing, estimates of traffic loads over any navigation point or ATC sector can be provided. Discussions are initiated with all the partners concerned (states and aircraft operators), starting each year in October and ending in February. The outcome of this planning is the Traffic Orientation Scheme, which dictates the routes to be used by operators when planning flights from specific departure areas to specific destination areas during the coming summer (Martin, 1993).

Pre-tactical ATFM on regional scale (1 day lookahead): pre-tactical activity is directed at the specific situation one day ahead. On the basis of updated demand data (incorporating Repetitive Flight Plans (RPLs) and last minute changes notified by aircraft operators), archived data of traffic situations on a similar day in the recent past, and taking into account the latest information about capacity in the Area Control Centers (ACCs), a pre-tactical ATFM plan for the coming day is developed. This plan, which defines the restrictions to be applied to traffic flows on the day concerned, is published every day around noon in the form of an ATFM Notification message (ANM) and is dispatched to more that 1000 addressees (Air Traffic Services and Aircraft Operators). The ANM describes in a single message all the tactical ATFM measures which will be in force on the following day (Martin, 1993).

Tactical ATFM on regional and Flight Information Region (FIR) scale (several hours lookahead): on the day of operation itself the Flow Management Units (FMUs) will apply the measures announced in the ANM and will monitor whether the pre-tactical plan is having the desired effect. At the present time, tactical ATFM is based on the application of acceptance rates, expressed in terms of the number of flights per unit time that will be allowed to enter a specific congested area from a particular area of origin. Aircraft which plan to fly through a congested area – as detailed in the ANM – are expected to request a slot from the appropriate FMU. Slots are allocated mainly in the form of a revised departure time but sometimes as a time of arrival at an en-route point (Martin, 1993).

Air Traffic Control (ATC) Area Management on sub-FIR scale *(1 – 2 hours lookahead)* corresponds to operational supervision and tactical Airspace Management (ASM). This activity is responsible for dealing with events having a significant effect on traffic handling and throughput (such as NOTAMs, system failures, changes of airspace, airport and runway availability, meteorological hazard or traffic overflow). It adapts the sectors, selects the overall strategy for dynamic routing, airspace use, traffic segregation and runway usage in order to meet the strategic regulation plan (tactical ATFM plan) and the required capacity of the involved sectors. This includes assessing and smoothing the center's workload for the coming hours.

Planning ATC on single or multi-sector scale (20 – 30 minutes lookahead): serves to organise the traffic entering and leaving the planning area so as to avoid unmanageable situations inside the planning area (from a flight safety, flight economy and an ATC workload point of view). This involves aircraft sequencing, allocation of runways, routes, levels, delays and coordination with adjacent planning areas in order to establish agreed transfer conditions. The resulting plan must include a certain contingency to give Executive ATC the "manoeuvring liberties" needed to resolve unexpected problems.

Executive (tactical) ATC on single-sector scale (5 – 10 minutes lookahead): is responsible for implementing the plan established by planning ATC while maintaining satisfactory levels of safety (through separation assurance and aircraft guidance). The provided separation and aircraft guidance has to meet certain legal requirements (minimum separation values which depend on geographical, technical and institutional circumstances). Executive ATC has to monitor a highly dynamic system where the nature of the problems at hand can significantly change in the course of a few minutes. The resources available for problem solution are limited, and there are hard real-time constraints for the control loop which must detect these problems, develop solutions, and implement those solutions.

ATC Safety Net layer on single aircraft scale (2 minutes lookahead): complements the Executive ATC with functions such as Short Term Conflict Alert (STCA) and Minimum Safe Altitude Warning (MSAW). The purpose of this layer is to catch those safety threatening situations which were not resolved by the Executive ATC layer.

This hierarchy of layers can be continued to shorter and even negative time horizons (in this case the term "planning layer" is not appropriate any more).

Real-time operations layer on single aircraft scale (real-time): the physical act of communicating clearances, instructions, advice and requests to individual aircraft, executing procedures and changing the internal state variables of the ATM system as a reaction to the occurrence of triggering events (this progresses the chain of events). Real-time operations are what an incidental visitor sees happening when he/she observes a controller on duty. The incidental visitor would not see the meaning (all the tactical and strategical considerations) which are behind the observed real-time operations.

Forecasting and extrapolation layer *(past situations extrapolated to a target time, i.e. to real-time or to the future)*: serves to produce assumptions about the state vector of the relevant objects (individual aircraft, weather phenomena, the traffic flow, etc.) based on a description of the situation in the past (obtained via the history data collection layer). The purpose of forecasting and extrapolation is to close the feed-forward loops by transforming history data into a state

which matches the time horizons used by the various higher planning layers. Forecasts and extrapolations may be deterministic (with reduced accuracy of extrapolated state variables) or probabilistic (if the target time is too far ahead of the recording time). A track extrapolation 10 seconds ahead is an example of deterministic extrapolation, and a two-day weather forecast an example of probabilistic forecasting. Note that forecasting and extrapolation are to be distinguished from prediction based on an object's intentions (such as the planned trajectory or the clearance of a flight).

History data collection layer (negative time horizon, i.e. delayed): this is called surveillance data acquisition in the ATC context. It serves to create an accurate recording of the air traffic situation (or weather situation, etc.) over time. The obtained accuracy depends on the sensors used. The average age of the most recent data (the delay) depends on the sampling rate and the processing/communication delay. The data may be used in real-time for planning and control purposes (after extrapolation), or for off-line applications (route charges, accident/incident investigations, statistics, etc.).

Operational Concept for Flight Operations Management

The Flight Operations Management Operational Concept is a layered model quite similar to the ATM Operational Concept. Aircraft Operators are faced with managing the three main phases of aircraft operations: flight time, taxi time and turnaround time in preparation of the next flight. Each of these phases is managed in a number of planning layers and properly coordinated with the other phases. To illustrate the similarity with the ATM planning layers, here is a typical list of planning layers for the flight phase, as applicable to a scheduled airline:

- longterm strategic planning, to determine business opportunities and decide between fundamental options (10 – 15 years lookahead)
- aircraft fleet planning (5 – 10 years lookahead)
- acquisition and planning of commercial routes and destinations (several years lookahead)
- development of timetables for the coming season (6 months – 1 year lookahead)
- negotiation of routes with strategic ATFM (6 months – 1 year lookahead)
- filing of Repetitive Flight Plans (RPLs) (approx. 6 months lookahead): strategic flight planning: determination of aircraft maintenance schedules and initial allocation of resources to individual flights (aircraft, crew, logistics etc.) (approx. 3 months lookahead)
- tactical flight planning for individual flights, based on pre-tactical ATFM (1 day lookahead)

- Direct flight planning (off-board crew activities), based on latest NOTAMS, actual weather forecasts, cabin briefing etc. (45 – 60 minutes before scheduled departure time, lookahead until a few hours after scheduled arrival time).

- Direct flight planning (on-board crew activities), based on load sheet, ATIS etc. This results in completed fuel order, computed take-off data, planned 4-D trajectory, estimated time en-route (ETE), etc. (15 – 45 minutes before scheduled departure time, lookahead until scheduled arrival time).

- Strategic flight management is the coordination with ATC to obtain pre-departure clearance (PDC), including a departure slot, and other flow restrictions. Adjust planned 4-D trajectory accordingly. This corresponds to decisions made by tactical ATFM. Subsequently obtain start-up approval (5 - 15 minutes before "Off Blocks").

- Pre-tactical flight management: obtain expected clearances for departure, en-route, climb, descent and approach, and adjust planned 4-D trajectory accordingly. This represents coordination with decisions made by the Planning ATC layer (during taxi and flight, 30 minutes lookahead).

- Tactical flight Management: obtain actual clearances for push-back, taxi, take-off, departure, en-route, climb, descent, approach, landing and taxi, and adjust planned 4-D trajectory accordingly. This represents coordination with decisions made by the Executive ATC layer (from 5 minutes before "off-blocks" to docking and engine shut down, 5 – 10 minutes lookahead).

- Prepare execution of tactical manoeuvres, based on the latest 4-D trajectory plan and tactical ATC instructions (vectoring). This represents execution of cockpit procedures and coordination with decisions made by the Executive ATC layer and the ATC Safety Net layer (during taxi and flight, 30 seconds to 2 minutes lookahead).

- Prepare execution of collision avoidance manoeuvres, based on visual observations and/or ACAS/TCAS (during taxi and flight, 5 – 30 seconds lookahead).

- Real-time operations layer (real-time): the physical act of operating (controlling) the aircraft and manoeuvring it in accordance with the most up-to-date 4-D trajectory plan, and the act of communicating with various partners such as ATC.

- Forecasting and extrapolation layer (past situations extrapolated to a target time, i.e., to real-time or to the future): for example, dead-reckoning techniques, fuel burn prediction, and other estimations.

- History data collection layer (negative time horizon, i.e. delayed): for example, flight data recording and navigation data acquisition.

Planning Theory For Operations

The foregoing describes the functioning of "layered" ATM and Flight Operations Management in specific (operational) terms. The advantage of this approach is that it is pragmatic and permits the reader to relate the story to his or her own operational experience as opposed to being theoretical. The disadvantage is that the same basic operational problems are unknowingly solved over and over again, for different lookahead time scales, in different terminology, and by people with different backgrounds.

Now this section of the paper addresses issues such as:

- the different goals that may be set in an automation strategy (these goals are heavily influenced by human factors)
- the development and assessment of certification strategies for operations management

Thus for certification purposes, we need a kind of theoretical insight into this "layered" planning technique. What is called "planning theory" in this paper represents an attempt to identify some of the basic underlying principles in the operation of an Air Transport System. The subject of planning theory is now presented in the following.

The Players in Operations Management

The Air Transport System. The Air Transport System is the domain of interest of this paper. The generic term *Air Transport System* refers to the aggregate of weather, airspace, aerodromes, aircraft, aircraft operators (commercial, military, general aviation and aerial work) and ATM/CNS (Air Traffic Management/Communication Navigation Surveillance) Systems, all operating together in a particular geographical region.

Actors. In accordance with the above definition, the Air Transport System consists of a number of interacting elements, such as airlines, aircraft, pilots, airports, runways, airspace, routes, ATC units, controllers, systems, weather phenomena, aircraft separation etc. For the sake of generalisation, I will call these elements the *Actors* of the Air Transport System.

Relationships between Actors. The operation of the Air Transport System is far more than the sum of the operation of the individual Actors. Indeed, these Actors are in constantly changing interaction with each other. Managing the operation of the Air Transport System means managing these interactions. Some interactions are to be promoted because they are necessary ingredients of the proper operation of the Air Transport System. Others represent problems, and system management efforts are directed at avoiding or removing such interactions. An example of the latter is the separation conflict between two aircraft. Some of the most important general types of interactions (relationships) are:

- *User/resource relationship:* Actors in a resource role exist in limited supply with a variable number of Actors in a user role competing to use that supply (establish a user/resource relationship). Examples are: aircraft operators with respect to aircraft, aircraft with respect to runways, clients with respect to database servers, aircraft with respect to route capacity, aircraft with respect to mutual separation, flights with respect to ATM, etc.

- *Competitor relationship:* users competing for the same resource are in a competitor relationship. Examples are: two aircraft approaching the same airport at the same time, two VHF radios attempting to transmit on the same frequency at the same time, areas of severe weather with respect to aircraft wishing to use that same airspace, etc.

- *Collaborator relationship:* resources able to distribute the user load between them (i.e. to reduce bottlenecks) are said to be in a collaborator relationship. Examples include: parallel runways, different flight levels, parallel routes, main vs. reliever airports, etc.

- *Buffer relationship:* resources able to temporarily absorb the user load of another resource are called buffers. Examples are holding patterns, route extensions, queues, contingency measures, etc.

- *Control relationships:* sometimes Actors are responsible for the operation of another Actor. This responsibility may range from defining an operating envelope (providing policy, guidance, operating constraints, or allocating workload), to assuming detailed control. Examples: pilots with respect to aircraft, controllers with respect to controlled flights, Air Traffic Flow Management (ATFM) with respect to Air Traffic Control (ATC), etc.

- *Target relationships:* when Actors are planning to reach a goal, actor and goal are said to be engaged in a target relationship. Example: a flight with respect to its destination airport.

- *Part-of relationship:* indicates the (permanent or temporary) assembly of individual actors into a composite system, having a certain state vector in common (such as a runway is part of an airport, a pilot is part of an aircraft in flight).

The Environment. In simple terms, the environment of an actor is everything that surrounds that actor. However, only that part of the environment is relevant with which the actor interacts in one way or another.

This leads to the following natural definition of environment: the total set of existing, expected and planned relationships with other actors. The environment is dynamic because the membership of this set is subject to change as time elapses: relationships disappear and new ones come into existence.

The Conduct of Operations

Operations in a World Without Planning. Object-Oriented Analysis (OOA) techniques such as Coad and Yourdon (1991) and Shlaer and Mellor (1992) describe the world in a mechanistic manner as a set of objects (actors), with predefined relationships, predefined life cycles (state transition diagrams), predefined event chains and communication capabilities.

This may perfectly suit the needs of system analysis for the purpose of developing static (non-adaptive) pieces of software or analysing rigid organisations (mechanistic systems), but it seems a bit inadequate for documenting the operation of complex goal oriented systems such as the Air Transport System.

OOA may correctly capture such a system on a syntactical, real-time operations level (existence of Actors, possible relationships, state transitions, etc.), but it misses out on the semantics (the whole layered planning process preceding the physical conduct of operations).

Operations in a Goal Oriented World. In contrast, the operation of the Air Transport System is highly adaptive (i.e., it is governed by a set of constantly *modified* and *(re)created* scenarios, scripts, procedures, project plans, flight plans, story boards, event models, rules, regulations, strategies, tactics, philosophies, etc.). This modification and (re)creation is the above mentioned layered planning process which precedes the physical conduct of operations. It happens this way because most of the actors in the Air Transport System are goal oriented entities. In order to reach a goal in a world full of uncertainties and conflicting requirements, one needs to plan the future and reduce the amount of improvisation. In fact, all the actors of the Air Transport System spend a considerable part of their energy on such planning activities.

So what are these planning activities all about, in a nutshell? They are about developing a scenario, refining and finally executing it, in an environment of external and self-induced perturbations.

The external perturbations are the unforeseen events, interactions and timing in an actor's environment. External perturbations occur because the environment may be inherently unpredictable, but also due to lack of overall coordination in the Air Transport System. The self-induced perturbations come from an actor's inability to accurately execute his or her own operational scenario. These are cases of mismanagement, in the operational sense. On top of that, the Actor may simply be following a bad scenario (e.g. with lack of feasibility and full of inconsistencies). This type of problem and the perturbations give rise to the need for constant situation assessment and revision of the scenario.

Fuzziness in the Planning Process. Actors deal with two types of scenarios: probabilistic and deterministic. The countdown towards the moment of physical execution of a particular operation is normally spent in different *uncertainty phases:*

- *PHASE 0*: the need for the operation has not yet been identified
- *PHASE 1*: the need for the operation is identified, including an approximate target time, but no plan or scenario is available
- *PHASE 2*: the phase of fuzzy and probabilistic scenarios
- *PHASE 3*: the reduction of uncertainty, to transition from fuzzy and probabilistic scenarios to a very limited number of candidate scenarios (scripts)
- *PHASE 4*: the phase in which one of these candidate scenarios has achieved a very high probability of occurrence, and has become a structurally stable script for the operation ("structurally stable" means that sequence of events is stabilised, and partners for various types of relationships are known, e.g. "contractual" status of relationships are established)
- *PHASE 5*: the phase in which the script does not structurally change, but the accuracy of its various parameters (such as timing, planned value of state vector, details of interactions with other Actors) is improved

- *PHASE 6*: the actual execution of that script, resulting in a physical operation (the chain of events is progressed)
- *PHASE 7*: the phase where factual data on what has happened is not yet available
- *PHASE 8*: the availability of history data describing what actually happened

To visualise the relationship between these uncertainty phases and time, an uncertainty-time diagram is used in this paper. The time axis is to be seen as absolute time; and the uncertainty axis lists the above phases to give a qualitative idea of the accuracy of a given scenario.

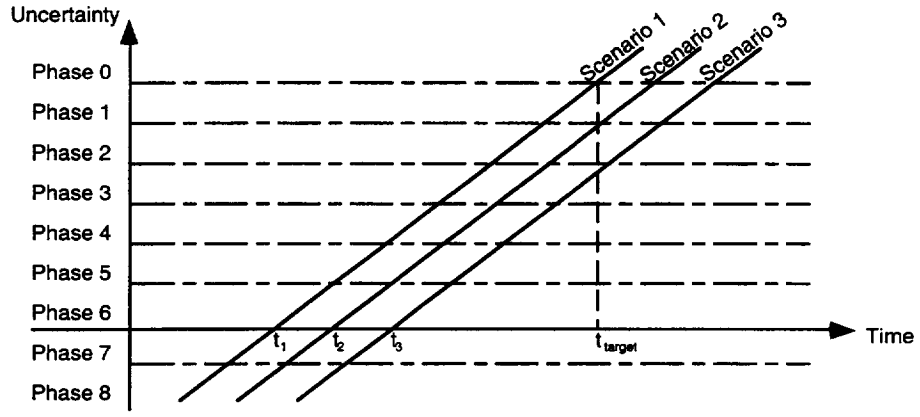

Figure 1.

Figure 1 illustrates the production of different versions of a scenario. Scenario 1 is associated with time t_1, scenario 2 with time t_2, etc. These reference times correspond to the real-time execution of what is spelled out in a particular scenario version. In the example of scenario 1, the part before t_1 is history, and the part after t_1 is the plan for the future. An example will clarify this. A flight plan is to be seen as a scenario. At time t_1, part of the flight has been completed already, the next leg is quite accurately planned, but the details of arrival are uncertain. For example, because of the unpredictability of the weather it is uncertain whether the alternate destination will have to be used or not.

This story can also be looked at from the perspective which is so well known from space vehicle launches: the countdown view. While counting down, a particular time target in the future (such as the time of arrival of a flight) is associated with different scenario versions as time elapses. Each new version is more accurate with respect to time target because prediction is less of a factor.

Figure 1 also illustrates that each scenario version is structured in a particular way: it is accurate in the short run and exhibits properties of the earlier fuzzy phases the further it looks into the future. It is important to note that Actors do quite a lot of planning and reasoning while still in the phase of fuzziness.

All this explains why operations management works as a "rolling program" of scenario development. In this approach, a particular situation at time target seems to be planned in an iterative fashion because it is associated with a number of different scenario versions. On the other hand, the planning process chases a moving time horizon because the subsequent scenario versions are time stamped differently, but must maintain the same outlook with respect to their time stamp.

This scenario revision process is implemented by a control loop. In project management, the control loop is called the *PDMA-cycle* (plan-do-monitor-adjust). In ATM, one usually distinguishes the following phases (Eurocontrol, June 1992; EATCHIP Task Force on ATC System Integration, June 1992):

- acquire information
- monitor current situation
- predict evolution
- identify problems
- propose and evaluate solutions
- choose solution
- communicate and implement solution.

Each cycling through these control loop phases produces a new version of the scenario. But let us return to the previously mentioned hierarchy of uncertainty phases. In system terms, this hierarchy could be expressed as the following strategy:

- determine the desired start state and end state (goal/target) of the operation
- plan the time of occurrence for start state and end state
- select intermediate states (sub-goals)
- determine the order of intermediate states (temporal organisation of activity)
- elaborate synchronization and coordination requirements for the operation (type and sequence of the relationships needed or expected during the operation)
- determine the partners for these synchronization and coordination relationships (production of a structurally stable script, establishment of "contractual" relationships with partners)
- work out the timing (start to end) of the synchronization/coordination with each of the above partners
- determine the detailed timing (accuracy) for the intermediate states
- operate in real-time, i.e. perform state transitions and interact (exchange events) with various synchronization/coordination partners
- collect history data.

Take any type of operation, say ATFM, planning ATC, flight planning, flight management, project planning, and it is possible to express the operations planning in the above terms. A third way of expressing this strategy is reflected in the traditional *WHAT-HOW-WHERE-WHEN* sequence:

- the *WHAT* phase identifies the operation
- the *HOW* phase is responsible for identifying the needed interactions
- the *WHERE* phase produces the stable script which identifies the partners for the individual interactions
- the *WHEN* phase puts on the accuracy by refining the timing.

One can continue repeating this strategy in different terminology disguises. In a systems development context this "scenario development strategy" is called a life cycle:

- user requirements definition
- operational concept definition (sometimes termed requirements analysis)
- operational requirements definition (also called system requirements definition)
- architectural design (alias technical concept definition)
- detailed design
- system procurement and installation
- system operation.

In project management terms, the hierarchy looks as follows:

- state the overall mission of the project
- determine the completion date of the project
- develop the work break-down structure (WBS)
- identify the interdependencies between work packages (production of Pert Chart)
- perform rough allocation of the total project duration to individual work packages (production of initial Gantt Chart)
- allocate resources to work packages
- refine timing of work packages by eliminating resource over-allocation (production of Gantt Baseline Chart)
- adjust the project plan based on plan deviations
- execute the project plan
- do progress tracking.

All these strategies are nothing more than variations on the same basic theme. Depending on the complexity of the operation and the expected number and magnitude of perturbations, the length of this countdown process – alias planning strategy – may take just a few seconds, and on the other extreme several years or even decades.

The Feasibility of a Scenario. The objective of each layer (or countdown/anticipation phase) is to deliver an acceptable situation to the next lower layer. This means: maintaining a set of conditions (i.e., a "solution space" or operational performance envelope) in which one or more feasible action plans exist. If the higher layer fails to maintain those conditions, the lower layer might not be successfully completed. The expression "to pass the point of no return" emphasizes the timing and state transition aspects of this feasibility collapse.

Consequently, one of the responsibilities of a higher layer is to maintain a constant awareness of the operational performance envelope of the next lower layer. The ATC concept of "minimum legal aircraft separation requirement" is an example of such an operational performance envelope. The above mentioned feasibility collapse may have internal and external (environmental) causes. A mistake in the calculation of aircraft endurance during flight planning is an example of an internal cause. So is the failure of a pilot to initiate the landing flare at the right moment, or the failure of a controller to detect a loss of separation between two aircraft. An unexpected weather change to IMC (Instrument Meteorological Conditions) during a VFR (Visual Flight Rules) flight is an example of an external cause.

The Impact of Perturbations. As mentioned, there is a constant need for situation assessment and revision of the scenario due to internal and external perturbations. In addition, the notion of "operational performance envelope" has been introduced.

The impact of perturbations depends on the magnitude of those perturbations. In this context, "magnitude" can refer to size as well as duration. If the magnitude of the perturbation exceeds the operational performance envelope of the planning layer under consideration, then there is nothing this planning layer can do to solve the problem. It is up to a higher layer to take care of the situation. That, of course, cannot be done in a reactive way after the problem occurred. By virtue of its longer planning horizon, the higher layer is supposed to have prevented the problem.

If the magnitude of the perturbation does *not* exceed the operational performance envelope of the planning layer under consideration but it exceeds the envelope of the next lower layer, then this planning layer is responsible. It has to modify the scenario within the possibilities of that particular planning horizon.

If the magnitude of the perturbation does not even exceed the operational performance envelope of the next lower layer, then this planning layer does *not* have to change the scenario with respect to that particular planning horizon.

Whatever layer is responsible, in a properly functioning system the problem is solved in anticipation (a certain time before it would actually occur). This can be seconds, minutes, hours, days or even years in advance. Additionally, this revision of the scenario by a particular layer invalidates all the plans under the responsibility of lower layers. This imposes certain time constraints on the lower layers which have to recreate their part of the scenario from scratch. Indeed, imagine the situation in which there exists a sufficient number of possible solutions on the shorter planning horizons, but the responsible human or machine is unable to produce these solutions in the available time. An example of this is the situation where the pilot "doesn't keep up with the airplane": he or she is overtaken by events rather than staying abreast of them.

The Impact of the Environment. In order to plan the scenario of an Actor with a certain accuracy to a certain time horizon, the predictability of the environment must be equal or better than the fuzziness/accuracy of the desired scenario.

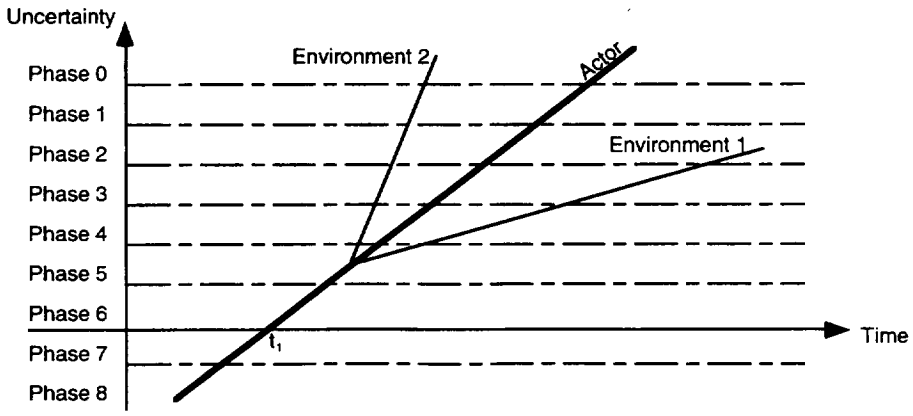

Figure 2.

This is illustrated in Figure 2. The scenario labeled "Actor" can be implemented in environment 1 but not in environment 2.

Let us illustrate this with the example of planning a conflict free 4-D tube clearance (the "Actor" scenario) in a given environment of other aircraft trajectories. The bottleneck of the planning process is the part with the greatest uncertainty. Uncertainty translates in this example into planning horizons, time windows (departure, overflight, climb, descent, arrival), positional accuracy and confidence levels.

Assume the following operational goal for the Actor: touchdown within 30 seconds of exactly 2 hours. Of course the Actor needs to have the capability to execute this scenario with the required accuracy. It is intuitively clear that it is feasible to plan this in an environment number 1 where the landing times of the other aircraft will occur with an accuracy of 10 seconds. It is equally obvious that such planning is pointless in an environment number 2 where the landing times of the other aircraft will occur with an uncertainty of 5 minutes, unless the minimum separation values (safety margins) are greatly increased, with a resulting reduction of control capacity.

The Impact of a Lack of Knowledge. The role of knowledge is quite similar to what was said about the environment. Note the choice of words in the previous example: "will occur with an accuracy of". If I replace this with the words "is known with an accuracy of", we see the impact of a lack of information.

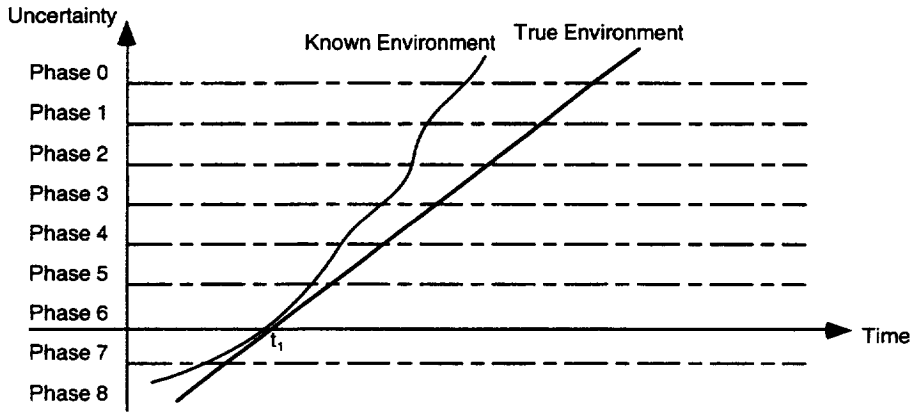

Figure 3

Figure 3 illustrates that the environment is assumed less deterministic than it really is, due to insufficient information. The Actors in the system have a lack of situational awareness, which translates into reduced planning horizons (the horizontal delta on the diagram) and reduced certainty at a particular outlook time scale (the vertical delta on the diagram). In plain words, the planning can only be as accurate as the knowledge on which it is based.

The attempt to approximate the inherent unpredictability as much as possible is the reason why future Operational Concepts strive to use better surveillance, better coordination and higher levels of system integration – air/ground integration and use of data link in particular.

Lack of Correlation with Reality. The other extreme is a lack of correlation with reality: sophisticated models of the future which make the Actors believe that the situation is very much under control.

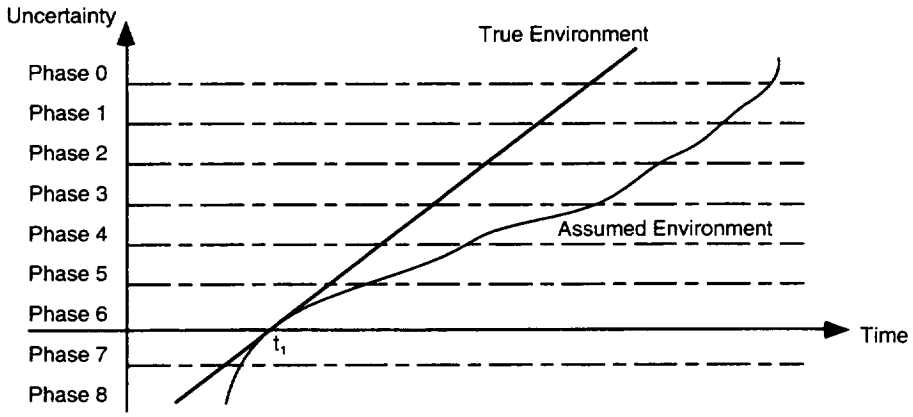

Figure 4.

That situation is represented in Figure 4. The description of the future is too precise: it is a collection of unfounded assumptions which will probably turn out to be false. For example, an ATC system which "sells" the idea that the next separation conflict of aircraft X will be with aircraft Y, whereas at the given moment it is inherently impossible to say whether it will be with aircraft Y or Z. A system acting like this will either fail or at least exhibit very poor performance because each such case of "over-confidence" probably creates a mistake.

The Need for Planning. Orville and Wilbur Wright did not need air traffic control in 1903. They certainly did not have any use for flow management. There seems to be a tendency that systems evolve to loose their simplicity over time (people call this "more advanced"): the environment becomes more complex, the system's internal complexity increases, the operation needs to be more optimized, uncertainty is less and less acceptable, and the operational performance envelopes are extended to enable the previously impossible. What used to be simple now requires advanced and accurate planning: no more "flying by the seat of the pants". This is now "follow the procedures" and "fly by the numbers". There was a time when aircraft flew but ATC did not exist, then a time with ATC but without planning controllers, and finally there was a need for ATFM (which is of course fairly recent).

In the future, one might see the beauty of Air Traffic Management: the completely deterministic Operational Concept with nearly 100% safety and nearly unlimited control capacity by virtue of highly accurate pre-planned (booked) 4-D conflict free flight trajectories from take-off to landing. You negotiate (book) a flight plan (all previously booked flight trajectories remain unchanged), and from then on everything unfolds like clockwork. Unfortunately, there are many uncertainties due to external events. Besides that, even if unexpected external events did not exist, operations managers on all planning levels might *want* to change their mind once in a while, instead of having to stick to plans which were cast in concrete long ago. A few things need to be remembered from the above:

- the need for planning tends to increase as systems, organizations and technology become more mature
- the stack of planning layers builds from the bottom up
- those higher planning layers always address the need for more global optimization of operations (the need for bird's eye views and crystal balls)
- the need for planning depends on the complexity of the operating environment (e.g. traffic density and geographical context)
- the need for planning depends on the complexity of the system (organisation and/or equipment) and the type of operation.

Optimization Strategies for Operations Management

What do goal oriented entities (humans, machines or composite systems) usually do to optimize their operations? A number of general strategies always return:

- have a plan, as early as possible
- have a plan, as feasible as possible (maximize contingency)
- have a plan which includes a strategy for dealing with probabilistic situations
- re-assess and revise the plan as often as possible
- have a plan, as stable as possible (i.e., the revisions should be as small as possible)
- have the ability to (re)create a plan quickly (improvise if necessary), to minimize the time delay between the last situation assessment and the availability of the new plan
- have the ability to stick to the plan (a minimum of internal perturbations)
- solve problems (external perturbations) as early as possible
- solve problems (external perturbations) as thoroughly as possible (full impact analysis of solution)
- if there is a choice, operate in as stable an environment as possible
- if there is a choice, operate in as predictable an environment as possible
- if there is a choice, operate in an environment with the least number of interdependencies (low complexity environment)
- avoid the unknown, i.e. operate in as well known an environment as possible (maximize the available information)
- split the planning process into different concurrently operating layers with different responsibilities, based on the dynamics of the possible perturbations (work with a hierarchy of plans)
- know the true extent of all the performance envelopes (how far can you go on each layer without compromising safety)
- devise a proper filtering strategy to dispatch perturbations to the responsible planning layer (full impact analysis of perturbation): a dispatch to a layer which is too high leads to unnecessary re-planning; a dispatch to a layer which is too low leads to safety problems.

Certification Issues

How should planning theory (i.e., the above considerations of planning layers), control loop phases and performance envelopes be seen within the context of certification? Rather than trying to give a complete answer, this paper attempts to give a number of useful indications. Before going into details, however, let's clarify the used terminology.

Definitions

For the purpose of this paper, I assume the following definitions:

- *Verification* is a review process, to check the system requirements against their source. The validity of the requirements themselves is verified, to ensure that a system which would be built to satisfy these specifications would also be suitable.

- *Validation* is the checking of a system design against the requirements. It is the production of (formal or experimental) proof, serving to establish a measure of confidence in the correctness and effectiveness of important system features. Validation is performed "after the fact", as for example during acceptance tests.

- *Feasibility Study* is similar to validation, but different in the sense that it is done in the exploratory phase ("before the fact"), in order to select a suitable solution amongst different possible alternatives. A feasibility study never replaces validation.

- *Certification* is the administrative "rubber-stamping" of a validation, an endorsement to give it an official status and level of authority.

The Limitations of Certification

There is one catch in regard certification: the correctness and effectiveness of the certified system features (the fitness for operation) are not endorsed under unlimited operational circumstances. Every certified system or person "carries" a piece of paper which lists these circumstances and/or limits of authority: system or person such-and-such is certified to deliver operational performance X during a period Y under operational circumstances Z. In fact, these limitations can be equated to the "operational performance envelopes" which were introduced earlier in this paper.

Certification of the Planning Process

Normally, Operational Concepts are not certified in their totality, probably because that is beyond today's state of the art. However, there is a need to develop, validate and certify the standards and recommended practices which are used in support of Operational Concepts.

Traditionally, certification was focused on systems (equipment or humans) in order to qualify their functional capabilities and operational performance. Emphasis always seemed to be on the *real-time* operational performance (uncertainty phase 6 in the diagrams of this paper), because that is the easiest to observe and, more importantly, because it represents the ultimate judgment on proper operation of the system. It is the stuff the whole operations planning process is finally all about.

Now, systems become more complex and rely more and more on planning (automated or human). This means that it is no longer sufficient to certify that "the system works", regardless of how it achieves this goal. The planning process itself needs to be certified because it determines those situations in which a system will and will not work. As mentioned earlier, the documentation of these limitations is a crucial element in certification.

In other words, the time has come to consider planning layers and their individual control loop phases as objects for certification, instead of just physical people, equipment, functions and procedures.

After having said this, it must be clearly stated that planning layers and control loop phases already exist in today's systems because all kinds of functions and responsibilities fulfill these roles. But these functions and responsibilities have not been consciously designed based on sound planning theory. Instead, they historically evolved in a bottom-up fashion, over many system generations, just as language is a product of history rather than a "careful design". Thus the certification problem is considered to be twofold:

- certify the operational principle (i.e. the effectiveness of a certain combination of planning strategies)

- certify the implementation (i.e. the functions, responsibilities, etc.) of these planning strategies to certain performance standards.

Let us rephrase this in a bit more detail:

- Operations management uses a layered planning process which includes strategies for the reduction of uncertainty and for dealing with perturbations. The performance of this planning process can be expressed as specified under "Optimization Strategies for Operations Management" and in terms of the uncertainty phases defined under "Fuzziness in the Planning Process" in this paper.

- The interoperability of these layers and phases depends on mutual awareness of operational performance envelopes (internal operation and expected range of external perturbations) plus proper matching of these layers and phases.

- Certification needs to concentrate on the effectiveness of these strategies (the quality of the produced scenarios) and on the interoperability of layers and control loop phases. The exact documentation of performance envelopes is a *key issue* in the certification process. This is the framework for certification of the *implementation components* of Operational Concepts, i.e., the functions, responsibilities and operational procedures.

- Large systems have many players: groups of people and automated systems operate together in teams to make collective tactics and strategies (planning layers and control loops) happen. This task sharing defines the information flows between people, on the

human-machine interfaces, and between automated systems. Different tactics and strategies require different information flows.

- Functions, responsibilities and operational procedures are the "bricks" for building the implementation of an Operational Concept. The above mentioned information flows are the cement which keeps the "bricks" together. The existence of these "bricks" is to be justified in terms of the certified planning strategy, and the role of existing "bricks" is to be mapped on the planning layers and their control loop phases. New "bricks" should be designed to fit specific niches in that framework of layers and phases.

- To make the implementation of an Operational Concept perform as intended, the individual "bricks" need to be certified to meet the requirements imposed by the previously certified interface and performance specifications of planning layers and control loop phases.

Human Factors

All the above considerations about planning layers, control loop phases, scenarios, performance envelopes apply to any goal oriented system. That, of course, includes composite human-machine systems.

In such a system, the planning responsibilities outlined in the Operational Concept are allocated to humans and machines. This can be done in a top-down fashion (in an arbitrary manner), or bottom-up, built around the human capabilities and the state-of-the-art of technology.

Many studies have investigated the role of the human. The human factors field aims at determining the automation environment in which the human performs best. This paper does not attempt to draw specific conclusions from the existing literature, but in the end various strategies are possible to integrate the human into an automated system, or to support the human with automated functions. One strategy may be to give the complete responsibility for some planning layers to humans, and automate the remaining layers. For example, in ATC, automate safety nets but keep executive control largely manual.

Another approach is to take the control loop of a planning layer, automate some phases and leave responsibility for others to the human. To use again an ATC example: automate the monitoring and problem detection phases, but keep the proposal and evaluation of solutions, and the decision making phases manual.

No matter whether a layered or phased automation strategy is chosen, it is necessary to correctly use the strengths and weaknesses of humans and machines. In other words: within the framework of layers and phases, find out whether the human or the machine fits the requirements best, in terms of monitoring capabilities, problem solving capabilities, memory, speed, assimilation, pattern recognition, span of attention, reliability, etc.

Thus, the human gets certain modular chunks (layers, phases) of the overall Operational Concept (the planning strategy as described above). The problems of human factors certification can then be seen as the certification of interoperability of these chunks with the overall Operational Concept. In that sense, the human role is no different from an automated function taking the same responsibilities. The performance needs to meet the requirements as foreseen for that particular responsibility within the context of the total planning strategy.

Conclusions

General

The paper suggests that the "tactics and strategies" notion is a highly suitable paradigm to describe the cognitive involvement of human operators in advanced aviation systems (far more suitable than classical function analysis), and that the workload and situational awareness of operators are intimately associated with the planning and execution of their tactics and strategies. If system designers have muddled views about the collective tactics and strategies to be used during operation, they will produce sub-optimum designs. If operators use unproved and/or inappropriate tactics and strategies, the system may fail.

The author wants to make the point that, beyond certification of people or system designs, there may be a need to go into more detail and examine (certify?) the set of tactics and strategies (i.e., the Operational Concept) which makes the people and systems perform as expected.

The collective tactics and strategies determine the information flows and situational awareness which exist in organizations and composite human-machine systems.

The available infrastructure and equipment (automation) enable these information flows and situational awareness, but are at the same time the constraining factor. Frequently, the tactics and strategies are driven by technology, whereas we would rather like to see a system designed to support an optimized Operational Concept, i.e., to support a sufficiently *coherent*, *cooperative* and *modular* set of anticipation and planning mechanisms.

Again, in line with the view of MacLeod and Taylor (1993), this technology driven situation may be caused by the system designer's and operator job designer's over-emphasis on functional analysis (a mechanistic engineering concept), at the expense of a subject which does not seem to be well understood today: the role of the (human cognitive and/or automated) tactics and strategies which are embedded in composite human-machine systems. Research would be needed to arrive at a generally accepted "planning theory" which can elevate the analysis, description and design of tactics and strategies from today's cottage industry methods to an engineering discipline.

Planning Theory

A theory based on planning layers, control loop phases, uncertainty phases and performance envelopes would provide a modular framework to the task of designing and documenting Operational Concepts (i.e., sets of tactics and strategies). The second half of this paper represents an initial attempt to highlight the key issues of such a theory. When such a framework is used, the benefits may spin off to the certification task. In addition, it will put the role and contribution of human factors into clear perspective.

OOA

A few references to OOA (Object-Oriented Analysis) techniques have been made in this paper. It is felt that OOA is too mechanistic; i.e., it misses some expressiveness when used to analyze

and document systems consisting of goal oriented entities. Planning theory could be a suitable candidate to remedy that problem.

Annex: The European Need For ATM Operational Concepts

Currently, a number of organizations around the world wish to bring Air Traffic Management (ATM) into the next century with significantly improved capacity, productivity and economy. To that effect some are conducting R&D programs and others are planning and procuring new systems which will still be in service after the year 2000.

Their vision of the future varies: from revolutionary to a more evolutionary approach. But even in the conservative case, everyone expects that due to the accelerated pace of technological innovation, Air Traffic Management will change significantly *more* in the coming ten to fifteen years than it did in the past half century.

The above explains today's interest in the development of the ATM Operational Concepts that are suitable for application in the period 2005-2015. To some degree, this paper has been written with the European ATM context in mind. Therefore it is useful to include a short overview of the activities going on in Europe (European Civil Aviation Conference, April 1990 and March 1992; Eurocontrol, June 1992).

The Transport Ministers of the European Civil Aviation Conference (ECAC) Member States, meeting in Paris on 24 April 1990 and in London on 17 March 1992, have noted the substantial growth which is forecast in air traffic demand in the ECAC area to the end of the century and beyond, and the considerable efforts which are being deployed to expand the system accordingly and to reduce air traffic congestion in Europe.

In order to unite and accelerate those efforts, the ECAC Ministers have adopted:

- the ECAC En-Route Strategy and action program to harmonize and integrate the operations of their air traffic control systems in the 1990's; and

- the ECAC Airports Strategy which will provide a concerted systems approach to the airport / air traffic system interface.

For these strategies, commonly known as the *ECAC Strategy*, the ECAC Ministers have adopted the following overall objectives:

- to urgently provide increasing airspace and control capacity, in order to handle the traffic expeditiously while maintaining a high level of safety;

- to improve the potential throughput of European airports and their surrounding airspace while maintaining safety and respecting the environment.

These initiatives will prepare the way for the introduction of a new generation of air navigation technology on the eve of the 21st century. To this end, the ECAC Ministers:

- have committed themselves to complete the phased action program for air traffic control which is the basis of the ECAC En-Route Strategy within a challenging but realistic time scale; and

- have resolved that the current program of research and demonstrations undertaken by Eurocontrol, the Commission of the European Communities (CEC) and ECAC Member States should be extended to cover new procedures and equipment required for air traffic management in and around airports.

Within the framework of the European Air Traffic Control Harmonization and Integration Program (EATCHIP), detailed planning is now well under way within Eurocontrol to give effect to the ECAC Strategy.

Meanwhile, the concept of a European Air Traffic Management System (EATMS) is seen as the 21st Century goal towards which the energies of Eurocontrol, the participating National Administrations and the European Industry should be focused. It takes into consideration those concepts that have already been accepted, FEATS, FANS, ECAC Strategy etc., and offers a method of *how* the future system would operate, given that the technology will be available. This concept will be developed as EATCHIP Phase IV evolution and implementation. Addressing the time scale 2005 - 2015, it will provide the basis for Phase IV of the ECAC Strategy and in particular for:

- adoption of a common functional model integrating the airborne and ground based components of the future EATMS;

- definition and implementation of advanced systems supported by extensive automation and enhanced data communications available via the Aeronautical Telecommunications Network (ATN).

But a common functional model and advanced systems are not enough. Before those can be defined, an agreement will have to be reached on the innovations which will be applied to the underlying Operational Concept (i.e., the tactics and strategies) of the EATMS. That requires proper attention to the Human Factors aspects of these innovations.

For the time being, no plans exist to *certify* the EATMS Operational Concept in its totality. However, various *validation* activities are foreseen, to be concluded by an Operational Concept demonstration program, scheduled near the end of the EATMS System definition and planning phase (which is planned to complete around the year 2000).

Disclaimer

The content of this paper expresses the opinion of the author and does not necessarily reflect the official views or policy of the EUROCONTROL Agency.

References

Coad, P., and Yourdon, E. (1991). Object-Oriented Analysis, Second Edition. Englewood Cliffs, NJ: Yourdon Press.

EATCHIP Task Force on ATC System Integration (1992). Open ATM System Integration Strategy (OASIS). EUROCONTROL Document 922011.

EUROCONTROL (June 1992). European Air Traffic Management System (EATMS) – Concept Document, Issue 1.1.

European Civil Aviation Conference (ECAC) (April 1990). Air Traffic Control in Europe – ECAC Strategy for the 1990s.

European Civil Aviation Conference (ECAC) (March 1992). Relieving Congestion in & around Airports - ECAC Strategy for the 1990s.

MacLeod, I. S., and Taylor, R. M. (1993). Does Human Cognition Allow Human Factors (HF) Certification of Advanced Aircrew Systems? In J.A. Wise and V. D. Hopkin (Eds.), *Human Factors Certification of Advanced Aviation Technologies*. Berlin: Springer-Verlag. [in press].

Martin, B., Central Flow Management Unit (CFMU), EUROCONTROL (February 1993). Progress through better Air Traffic Flow Management. ATC '93 Conference, Maastricht.

Shlaer, S., and Mellor, S. J. (1992). Object Lifecycles – Modelling the World in States, First Edition. Englewood Cliffs, NJ: Yourdon Press.