# Reliability analysis of air traffic control

Sven Ternov, MD
Institution of Design Sciences, Lund Institute of Technology, Lund, Sweden
Consultant, Swedish Civil Aviation Authority (ATCC Malmoe)
e-mail: sven.ternov@mailbox.swipnet.se

## Abstract

A reliability analysis was made for the process *air traffic control at the Area Control Centre (ACC) at the Air Traffic Control Centre (ATCC), Malmoe, Sweden*. The method is called disturbance-effect-barrier analysis (DEB-analysis). It is a proactive method for risk assessment, based on a process view on accidents. According to this view accidents are seldom the results of isolated operator errors. Instead accidents evolve due to latent system failures (weaknesses) and insufficient safety barriers, making the system intolerant against human errors, and provoking these errors due to poor design of the operator-system interface.
The DEB-analysis consists of a meticulous action sequence mapping, generation of hypotheses on disturbances, validation of these through observation and interviewing, analysis of effects on the system of the disturbances, and identification of latent system weaknesses and insufficient safety barriers as possible causes for negative system influence.

This analysis points to some latent system failures, amongst others, lack of clarity and implementation of some of the written procedures, ill-defined roles for watch supervisors, and the burden on cognitive workload in handling the Air Traffic Control Automated System (ATCAS).
The analysis suggests strengthening of some administrative safety barriers, for instance, counter reading from ATC (Air Traffic Control) to aircraft of flight level, and some technical barriers in the form of a medium term conflict alert, a clearance-transponder-check, and a system aid for the surveillance of conflicts.

The system is considered basically ”non forgiving” to its operators, with weak barriers between an operator error and system failure, i.e. loss of separation between aircrafts.
Quantifying the analysis by means of a good coverage local reporting system of incidents is discussed, and also how the analysis could be used during a development phase of new systems.

# Introduction

The analysis is based on a process model for accidents (Kjellén, 1984) according to which accidents seldom are the result of isolated operator errors but caused by a complex interaction between different weaknesses in the system (system weaknesses, or latent failures), and insufficient safety barriers in the system against erroneous acts (Reason, 1990; 1997). Often situational factors (so called "unhappy circumstances") are identifiable, and can explain why the accident took place in a particular situation. Situational factors will often be activators of the latent system failures.

Latent system failures can be, for instance, insufficient servicing of equipment, inappropriate or outdated equipment, insufficient introduction of new staff, and inappropriate adaptation of working tasks to human cognitive ability.

Latent system failures can exert negative system influence in different ways. Some examples are:

- They can act as error traps for the operator (ATCO), i.e. the system weakness can provoke an erroneous act (for instance an inappropriate design of the label shift at the quick look (XQL-) function in connection with hands-over procedure).
- They can prevent error detection, for instance time pressure in connection with control of flight level when the airplane calls.
- They can create a messy situation for the operator, thus depleting his/hers cognitive resources, and thereby preventing further problem solving in a safe way (for instance monitoring aircrafts on new equipment for approach control, feeding data in the ATCAS-system, or extensive communication on the interphone).

Barriers, or safety barriers, are different kinds of hindrances, built into the system. Their purpose is to catch operator errors before they influence the system or, even better, to prevent the operator from acting in an erroneous way (Ternov, 1999).
Barriers can be administrative, as for instance counter reading between ATCO's in executive and controlling positions, or technical, for example in a short-term conflict alert system.
Barriers can be weak/relative, or strong/absolute, depending on their ability to catch disturbances/erroneous acts. Administrative barriers are often weaker than technical barriers (Ternov, 1999).

Accidents in a process model are looked upon as a chain of acts-effects, transferring the system from a stable state to a state of lack of control. Finally, if the defence mechanisms are insufficient to counteract the negative impact on the system a state of loss of control will occur, and system failure is imminent.

In this study "accident", or unwanted event, is defined as *the loss of separation* between aircrafts.
However, the real unwanted event in the complete system, consisting of ATC-airplane, is *collision* between aircrafts.

Thus this analysis only addresses part of the system, the ATC part. This means that a loss of control state for the ATC component does not

necessarily imply a collision between aircrafts since the ”aircraft part” also contains safety barriers, for instance visual observation by pilots and airborne collision avoidance systems.

The aim with this study is preventive: To identify latent system weaknesses and insufficient safety barriers in the ATC system thus creating a platform for improving safety.

This study is part of a research project whose aim is to validate a method for reliability analysis of the interface between man and machine (system). The method has so far been applied to health care and nuclear power industry.

## Method and material

The method (DEB - analysis, Disturbance - Effect - Barrier analysis) emanates from a method used by the nuclear power industry to analyse accidents and incidents. In Sweden this method of analysis of occurred incidents is called MTO-analysis (Man- Technique-Organisation), (INPO, 1990).

The DEB-analysis though is *proactive*, i.e. there is no accident/incident involved. The idea is, so to speak, to be a step in front of the incident/accident.

The DEB-analysis is partly based on existing methods for proactive risk analysis, such as ”Error mode and failure analysis” and ”Action error analysis” (Harms-Ringdahl, 1993).

The DEB-analysis focuses in detail on operator actions during the process chosen for analysis.

The analysis includes a certain amount of quality system auditing (ISO 9000, 1996). Written procedures are examined for suitability for a certain task in the sequence of actions, and the implementation of the procedures are observed. As with all quality system audits the issue of management is addressed.

After having chosen a process to analyse the first step is to make a fairly detailed *action sequence mapping*, i.e. what are the operator actions during the different working task sequences? Which procedures (written or non written) are guiding the operator during these tasks?

The next step is to perform a *disturbance analysis*. For each action sequence the question is asked: What would happen if the operator does too little, too much, too late, does nothing, or does it incorrectly?
In this way a number of fairly theoretical hypotheses concerning process disturbances are generated.

In step three, these hypotheses are validated by interviewing the process owners, i.e. the operators, and, if applicable, by analysing incident /accident reports.

For the validated hypotheses a number of questions are addressed:

- Which effects on system performance might these disturbances have?
- Are latent system weaknesses identifiable as causes for these disturbances?

- Do safety barriers exist in the system, which prevent harmful system influence due to these disturbances? If not, how can such barriers be designed?

The ATCO's work tasks involve quick changes between different kinds of problem solving, often running these tasks in parallel. In order to accomplish an action sequence analysis it was felt necessary to describe the different work tasks in a number of *sub processes*.

A flow chart, "DEB-diagram", is the working tool for the DEB-analysis. In this, the actions sequences are plotted against a time axis. The results of the different steps in the analysis, described above, are written in columns under the action sequence, which has been analysed.

**Material**

The process chosen to analyse was the Air Traffic Control at the Area Control Centre of ATCC Malmoe, Sweden. Excluded was terminal control. Military air traffic, which is integrated at the ATCC Malmoe, was also excluded.

The gathering of data took place during December 1998 to January 1999. It consisted of sitting alongside different ATCO's, and a number of interviews with these, management, chairman for the local flight safety group and a system engineer.

A number of incidents (loss of separation) reported to the Swedish Air Inspectorate from ACC, Malmoe (n = 15), were analysed with an MTO-like method, and used for validating the hypotheses concerning disturbances.

# Results

**Process description**

The process "air traffic control at the ACC Malmoe" was described in the following sub processes:

- Handling of the air traffic control automated system (ATCAS)
- Planning
- Hands over procedure (HOV) for incoming traffic to a sector (or from a neighbouring FIR)
- HOV procedure for traffic leaving a sector (or Malmoe FIR)
- Minute-operative (basic scenario, static)
  - ◊ Prevention of conflicts
  - ◊ Surveillance of discovered potential conflicts
  - ◊ Solving of conflicts
  - ◊ Follow up of conflict solution

- Minute-operative (dynamic scenario)
  - ◊ Service to aircrafts
  - ◊ Flow of traffic in connection with start or approach
  - ◊ Approach Copenhagen Airport

- Relief of ATCO

Actions in these sub processes are seldom undertaken as an uninterrupted series. Typically they are carried out in parallel with actions from other sub processes.

**Disturbances**

The action sequence analysis for these processes contains 47 action sequences. In this section abbreviated examples will be given of the disturbance analysis for a few of the sequences in some of the sub processes.

Planning

When clearance (CLR) is revised via interphone between adjacent flight information areas (FIR) the changes are noted on the strip. The pilot, the ”old” FIR and the receiving sector in the new FIR can misunderstand the changes. The effect might be that the flight controller’s mental model of the airspace does not fit the real world. The aircraft might enter the sector at another flight level than expected.

The controller might detect the disturbance if he/she reads the label information (transponder information) concerning the actual flight level. Some of the analysed incidents hint that this safety barrier is not commonly used.

When entering a new sector the aircraft should, during the first radio call, according to procedures inform the sector of its actual flight level. According to standard phraseology the answer from the sector is ”radar contact”. This barrier could be improved if the flight controller reads back the flight level after having checked this against the flight level on the strip and the transponder label.

Therefore, a latent system weakness might be that the working task is not designed in such a way that this check can be carried out consistently.

A suggested safety barrier would be to routinely read back the flight level at first call from an aircraft into a new sector, after having checked the aircraft’s radio information concerning flight level against strip and label information.

Co-ordination and revision

Co-ordination and revision of CLR require that the ATCO constantly updates his/hers mental picture of the airspace. Failure to update creates a risk to fail to see a conflict.
Change in CLR can be documented incorrectly on the strip by either the ATCO in the executive position, or the ATCO in the planner position.

According to written procedures, a CLR made by, for instance the planner ATCO, must be acknowledged by the other ATCO, but as there is no fixed phraseology for this communication (as for communication between aircraft and ATC) this can be done in a less than appropriate way. At least one of the incidents with loss of separation demonstrates this.

Clear and correct strip information can be read incorrectly. The ATCO can be ”cognitive fixated” on his/hers original mental picture of the airspace, and dismisses new information. Aircrafts, for example, should normally enter Malmoe FIR from Oslo FIR at a certain flight level. On one occasion the aircraft did not, due to weather conditions. The revised CLR was correctly printed out on the strip at Malmoe FIR, and read by the ATCO, but he nevertheless placed the aircraft in his mind at the flight level he was

used to. It ended up with a loss of separation incident.

One possibility for the ATCO to catch these errors could be to consistently read back the flight level when the aircraft calls, after having checked this against the strip and the transponder label.

The ATCO might have perceived a CLR for vertical change of position incorrectly. An effect of this could be, for instance, an aircraft levelling at a lower flight level than believed by the ATCO. A consequent call from the aircraft after having reached the new flight level might act as a safety barrier against this error.

This administrative barrier can be reinforced with a technical barrier if the CLR is fed into the ATC computer and automatically compared with transponder information concerning actual flight level (Check-Transponder-Check, CTC). If a mismatch between CLR and flight level occurs the ATCO will get an alert from the system.

This barrier might catch errors in communication and comprehension but not errors in misinterpretation. If the ATCO has interpreted available information incorrectly, and subsequently made a wrong decision, i.e. issued an erroneous clearance, a CTC barrier will not catch this as there is no mismatch between CLR and the aircraft's flight level.

If this situation is allowed to develop, i.e. is not detected, it might end up with loss of separation. If the system has a short term conflict alert the ATCO may get one to two minutes to solve the situation, but it is tight playing, and not appropriate as the sole strong barrier between a mistake and loss of separation.

Instead, a better technical barrier could be in the form of a conflict aid device (CAD) in which the software extrapolates aircraft trajectories. This device should nicely and softly point out for the ATCO that he/she might get a serious problem with aircrafts A and B in x minutes unless the flight paths are changed.

Minute-operative, static scenario, prevention

Planned conflict solution is the ideal situation where conflicts are detected, surveyed and necessary measures taken so to expedite the traffic in an elegant, safe and smooth way.
A prerequisite for this is that the ATCO has a correct "start model" of the airspace, and that this model is continuously updated in a correct manner. This idyllic picture of the minute-operative activity is unfortunately subject to disturbances (misunderstanding and misinterpretation of information), the effect being that the ATCO's mental model of the airspace gets incorrect.
In these cases the minute-operative activity easily turns from *planned conflict solution* to *acute conflict solution*. This will place a heavy cognitive workload on the ATCO, and increases the risk that he/she might loose the general view of the airspace.

Minute-operative, surveillance

The ATCO scans the strip bay and radar picture continuously, looking for potential conflicts. He/she can for instance notice an aircraft crossing the

main stream of traffic is due in the sector. The ATCO makes a mental note to survey whether this aircraft might create a conflict situation. If the ATCO forgets to follow up on this it might end up with loss of separation.

There is really no safety barrier in the system against the ATCO forgetting. And sooner or later he/she does forget (which a couple of incidents show). If the aircraft's symbol could be marked on the radar picture, eventually together with a timer function, it should serve as an aid for the ATCO to check up on an observed potential conflict.

Minute-operative, dynamic, service

Change in CLR is given for reasons other than preventing or solving conflicts. Normally, they are also given as a service to the aircrafts, such as in direct routing, change in flight level due to weight conditions etc.

Every change in CLR means the ATCO has to update the mental model of the airspace and change pre-printed strip information. Every change increases the chance of forgetting, misunderstanding or misinterpreting the situation. The analysis of incidents shows that in 11 of 15 cases the ATCO themselves made changes in CLR, which later caused loss of separation, i.e. he/she failed to correctly update the mental model. In five of those cases (5/11) the change of CLR was a pure service measure.

Relieving of ATCO

The written procedures concerning relieving of ATCO's are inappropriately followed. The relief sequence is often carried out very quickly (in approx. 30 sec), not allowing sufficient time for the relieving ATCO to situationalise, i.e. he/she starts with a "non operational" model of the air, thus paving the road for a loss of separation situation.

# Conclusion

The ATCAS-strip system is efficient in transmitting static information to all involved FIR's and sectors. But ATC is not static but very dynamic (see for instance Smolensky & Stein, 1998; Bruce, 1993). Updating the ATCAS consumes valuable and limited working memory resources of the ATCO, and there is ample opportunity for misunderstanding or misinterpreting information.

Certain written procedures were not properly implemented in the studied system, in part due to lack of understanding for their importance by the ATCO's (for instance relief procedures)

Basically, the ATCAS system is considered fairly "non forgiving" toward the ATCO, i.e. it does not allow for errors before a system failure (loss of separation) can occur.

The analysis suggests the introduction of a number of strong, technical barriers such as a clearance-transponder check device, a medium term conflict alert (a short term conflict alert will shortly be fitted into the system) and a system aid for surveillance of potential conflicts.

A number of administrative safety barriers might even be introduced, such as read-back to the aircraft from the ATCO of the actual flight level, after having checked the label and the strip

Analysis of incidents with loss of separation suggest that the airspace might be presented incorrectly to the ATCO, giving intuitively understandable information on horizontal separation but not on the more important vertical (procedural) separation. In almost all the reported case, loss of separation occurred in connection with vertical changes of aircraft position, and errors in judgement of aircrafts' relative vertical positions. To which extent would a vertical presentation of the air have prevented these incidents?

A DEB-analysis is primarily a qualitative analysis. It could be quantified if the organisation in question has implemented an effective local reporting system of process disturbances. At the time of the study this was not the case for ATCC Malmoe. The unit had reported 12 cases with loss of separation during the year studied, which probably constitutes a very minor part of incidents where the processes deviate from the desired or expected course (of which a great proportion probably contains a potential for violation of separation). It is not possible to quantify the analysis based on these few cases. They can only be used for modifying the qualitative analysis.

At the Malmoe control centre an attempt is now being made to improve the local reporting of near misses, acute conflict solutions (without loss of separation) and other traffic situations "where things did not turn out the way we wanted them to do."

In June 2001 Sweden is changing the old ATCAS system for a new strapless system (S2000, AirSys) at the Malmoe and Stockholm ATCC's. This new system will more or less contain the technical barriers asked for in this analysis, i.e. there will be a clearance adherence monitoring function (CLAM), a route adherence monitoring function (RAM), a medium term conflict alert display and of course a short term conflict alert.

An increased degree of safety however, is dependant on a combination of tuning the system parameters, designing working procedures to fit the way the new system works, and implementing these procedures.

A DEB-analysis could be a tool in a test and development phase for maintaining and improving safety by disclosing latent system failures and inadequate safety barriers. It might prevent a number of incidents with loss of separation to occur before system weaknesses are identified. An analysis though, as described in this paper requires a working model of the new system, written procedures for the operations and trained operators to work the system. Thus, the analysis can be made only at a fairly late stage during the development phase, probably first when full-scale simulation is available. At this stage the analysis might be able to disclose man-system misfits before the system goes operative, and that is the intention concerning S2000.
It should be redone after the new system has been put into operation.

Again, an effective local reporting of process disturbances will greatly help to quantify the results. That is partly the reason that the Malmoe centre wants to implement and trim such a system now, in order that it will be part of the safety culture when S2000 is put into use.

Even if a "full" proactive DEB-analysis on S2000 is not possible for the time being, due to lack of requirements mentioned above, we try a more "reactive" modification by using currently reported incidents. We do a theoretical simulation of the cases in S2000, by asking, "how would the new system handle a similar situation?" and "will built-in safety barriers in S2000 catch errors and help avoid unwanted traffic situations?"
This has already raised a number of questions concerning potential system weaknesses and parameter settings, which previously have not been addressed.

## References


Bruce, D.S., Freeberg, N.E. An explanatory model for influence of air traffic control task parameters on controller work pressure. 1993: 37th annual meeting, Human Factors and Ergonomics Society, proceedings.

Harms-Ringdahl, L. Safety analysis- principles and practice in occupational safety. London, Elsevier Applied Science, 1993.

INPO (Institute of Nuclear Power Operations). Human Performance Enhancement System, program description. INPO document INPO 90-005, Atlanta, 1990.

ISO 9000 International standards for quality management, Stockholm, SIS förlag, 1996.

Kjellén, U. The deviation concept in occupational accident control-I. Accident analysis and prevention, 1984;16(4):289-306.

Reason, J. Human Error. Cambridge, Cambridge University Press, 1990.

Reason, J. Managing the risks of organizational accidents. Vermont, Ashgate, 1997

Smolensky, M.W., Stein, E.S. Human factors in air traffic control. San Diego, California, Academic Press, 1998.

Ternov, S. The human side of mistakes. In: Spath, P. (ed.) Error reduction in Health Care, Jossey-Bass, New York, 1999.

## Author presentation

The author is a physician, specialised in general medicine. For the last three years he has been engaged in research on human-system interface design at the Institute of Technology in Lund, Sweden. His special interests are system deviations in complex systems, and methods for identifying system weaknesses during accident investigations. He has been engaged in system analysis in health care, nuclear power, and for the time being, The Swedish Civil Aviation Authority (air traffic control).