Advances in Safety and Reliability – Kołowrocki (ed.)
© 2005 Taylor & Francis Group, London, ISBN 0 415 38340 4

Development of a causal model for air transport safety

B.J.M. Ale
Risk Centre TU-Delft, Delft, The Netherlands

L.J. Bellamy
White Queen BV, Hoofddorp, The Netherlands

R.M. Cooke, L.H.J. Goossens, A.R. Hale & D. Kurowicka
TU-Delft, The Netherlands

A.L.C. Roelen,
NLR, Amsterdam, The Netherlands

E. Smith
DNV, London, England

ABSTRACT: The development of the Netherlands international airport Schiphol has been the subject of fierce political debate for several decades. One of the considerations has been the safety of the population living around the airport. In the debate about the acceptability of the risks associated with the air traffic above The Netherlands the need has arisen to gain a more thorough understanding of the accident genesis in air traffic, with the ultimate aim of improving the safety situation in air traffic in general and around Schiphol in particular. To this aim a research effort has started to develop causal models for air traffic risks in the expectation that these will ultimately give the insight needed.

1 INTRODUCTION

As early as the beginning of the 1990's the Commission on Environmental Impact Assessment put in a plea for the development of a causal model for air transport safety. This model would, at least in principle, be better equipped to account for airport specific circumstances and measures than the risk assessment model currently in use, which is based on – selected – historical data.

Causal modelling is considered to be a powerful tool in supporting the insight into the interdependencies between the constituent parts of complex systems. As far as safety is concerned the propagation of fault situations can be modelled and followed. Weaknesses in protection against fault propagation can more systematically be determined. The power of causal modelling can be greatly enhanced if probabilities and logical dependencies can be quantified. The effect of safety measures or conversely the breach of safety barriers can then be evaluated quantitatively allowing comparisons between alternatives and cost benefit considerations.

Using causal models, policies and inspection regimes can be tailor-made to the vulnerabilities in the safety systems and to those activities that contribute significantly to the risk.

In the model the air-traffic system is considered from the point of view of air travel. This means that a successful flight from an airport of origin to an airport of destination is the activity of central concern. Building an aircraft, maintaining it, loading it, fuelling it, getting cargo and passengers aboard and guiding it through airspace all are considered as activities that are associated with this journey.

In previous attempts at modelling the risks of air traffic [Piers et al 1993, Smith 1998, Cowell et al 2000], the focus was on catastrophic events and in particular the crash of an airliner into inhabited areas. The current purpose is to describe the air traffic system and its safety functions in such a way that the relationship between the various components of the system and the management system in the model are sufficiently realistic as to make it possible to analyse risk reduction alternatives within a given system – such as an airfield – or differences between different systems. The model should have sufficient capabilities to allow quantification of these differences to support cost benefit comparisons.

2 AIRPORT PLANNING AND REGULATION

The national airport of the Netherlands was founded in 1925 in the north-eastern part of a former lake: the Haarlemmermeer. In the early days there were many kilometres of empty land between the airport and the nearest cities, Amsterdam and Haarlem, but these cities grew and so did the airport. In the mid seventies Schiphol was almost completely surrounded by buildings. In 1989 the discussion started about a further expansion of Schiphol Airport with at least one more runway. This would allow twice as many movements as there were in 1989 to be accommodated. In this discussion four environmental concerns were identified: noise, air pollution, odour and third party risk.

In support of decision-making on how to extend the airfield to accommodate the anticipated growth of the number of movements, an Environmental Impact Assessment (EIA) was carried out. In this procedure, which is required by law for major infra-structural developments such as airport expansions, studies were performed regarding, amongst others, the third party risk consequences of several airport development options. The concern about third party risk was intensified due to a crash of a cargo Boeing 747 into an apartment building in a suburb of Amsterdam, the capital of the Netherlands. In this accident, which happened on October 4th 1992, the four crew members were killed together with 39 inhabitants on the ground. Parliament was prepared to let Schiphol expand but insisted that the risks should not be larger than in 1990 and specified that a *statistical causal* model should be developed and used to show that its demands were met [TK 2002].

3 RISK ESTIMATION

The methodology for quantification of the external risks of air transport has been developed only recently. There are three main methodologies: the method developed by the Netherlands National Aerospace Laboratory NLR [Couwenberg 1994, Goudeleeuw 1995, Piers et al 1993], the method used by the National Air Traffic Services (NATS) [Cowell et al 1997, Cowell et al 2000)] and Aircrash, developed by Technica in London [Technica 1990, Technica 1991].

There are, however, limitations to these models, which makes their applicability restricted to statistical calculations of third party risk. These models can only take into account differences between general characteristics of airports such as their location in the world, or the volume of traffic [Ale 1998, Ale & Piers 2000].

For a more detailed and airport specific assessment of risks a more advanced understanding of the pathways to accidents, their probabilities and the consequences is needed. In the governmental document on safety policy in civil aviation (Veiligheidsbeleid Burgerluchtvaart) [TK 1996] of 1996, causal modelling is mentioned as one of the possibilities to achieve such an understanding. The Safety Advisory Committee for Schiphol which was appointed to provide the minister with advice on Schiphol Airport has also advocated the development of such a causal model [Hale 2001, Hale 2002].

Causal modelling is a powerful tool in supporting the insight into the interdependencies between the constituent parts of complex systems. Causal modelling has been the starting point for the modelling of failure mechanisms in Nuclear Power Plants [NRC 1975].

As far as safety is concerned the propagation of fault situations can be modelled and followed. Weaknesses in protection against fault propagation can be determined more systematically. The power of causal modelling can be greatly enhanced if probabilities and logical dependencies can be quantified. The effect of safety measures or conversely the breach of safety barriers can then be evaluated quantitatively allowing comparisons between alternatives and cost benefit considerations to be made.

Using causal models, policies and inspection regimes can be tailor-made to the vulnerabilities in the safety systems and to those activities that pose the most risk. The current project builds on demonstration projects performed by DNV and NLR earlier [DNV 2002, NLR 2002]. It will result in a working causal model containing the minimum of sub-system descriptions, data gathering and software development which is necessary to obtain results that are meaningful to gain insight into the working of the safety system of air transport and to obtain results that allow the development of improvement strategies.

4 THE IMPORTANCE OF CAUSAL MODELLING

Despite the impressive level of safety of today's aviation system, it is generally acknowledged that the accident rate has to be decreased further [FAA 1998]. The main reason is the projected growth in the number of air traffic movements. If the accident rate does not decrease, the growth of air traffic will inevitably lead to an increase in the absolute number of accidents, which is regarded by many as unacceptable. This has led to ways to *actively* pursue an increase in the aviation safety level by introducing risk assessments as an integral part of the design of the aviation system. In a design approach, the aviation safety level is considered an overall design requirement instead of an inevitable result of aviation activities. Risk budgets – how much every element maximally may contribute to the overall risk – can then be assigned to the various elements within the aviation system [CAA 2004, Gleave 2002, Federal Register 2000]. Assigning risk budgets to aviation elements requires an understanding of how the risks of individual elements in the system influence the overall level of safety. This implies knowledge of causal sequences of accidents and incidents. The design approach requires a transparent causal structure in a risk model that explicitly relates the overall level of safety to the level of safety of individual elements.

Like many other high-hazard, low-risk systems, the aviation system has developed such a high degree of technical and procedural protection that it is largely proof against single failures, either human or mechanical [Amalberti 2001]. The aviation system is more likely to suffer 'organisational accidents' [Reason 1990]. That is, a situation in which latent failures, arising mainly at the managerial and organisational level, combine adversely with local triggering events and with the active failures of individuals at the execution level [Reason 1997]. A causal model captures those failures and interactions qualitatively. How to quantify these is only partially solved [Bellamy et al 1999, WORM 2003] and further efforts are part of the current project.

A feasibility study on causal models for third party risk [Roelen et al 2000] provided a sound basis for the development of causal models associated with accident and incident analysis.

5 PREPARATORY PROJECTS

In the program to develop causal models two pilot projects have been undertaken. These were aimed at establishing the potential for these kinds of models and to determine whether there would be a preferred line of development. These projects were conducted by DNV [DNV 2002] and a consortium consisting of NLR, TU-Delft and the Aeromedical Institute [NLR 2002]. The former study was paid for by the ministry, the latter was funded by the FAA. Both projects resulted in demonstration versions of the models. The differences between the two approaches are in the causal model structures used (fault tree versus Bayesian belief nets), in the representation of management influences and in the way expert judgement is used in developing the necessary quantification data: the numbers. Since the approaches really are complementary the opportunity is taken to combine the two.

Central in the project is that the air-traffic system is considered from the point of view of air travel. This means that a successful flight from an airport of origin to an airport of destination is the activity of central concern. This is known as the gate to gate concept (Figure 1). Building an aircraft and maintaining it, loading it, fuelling it, getting cargo and passengers aboard, selecting and training its crew and guiding it

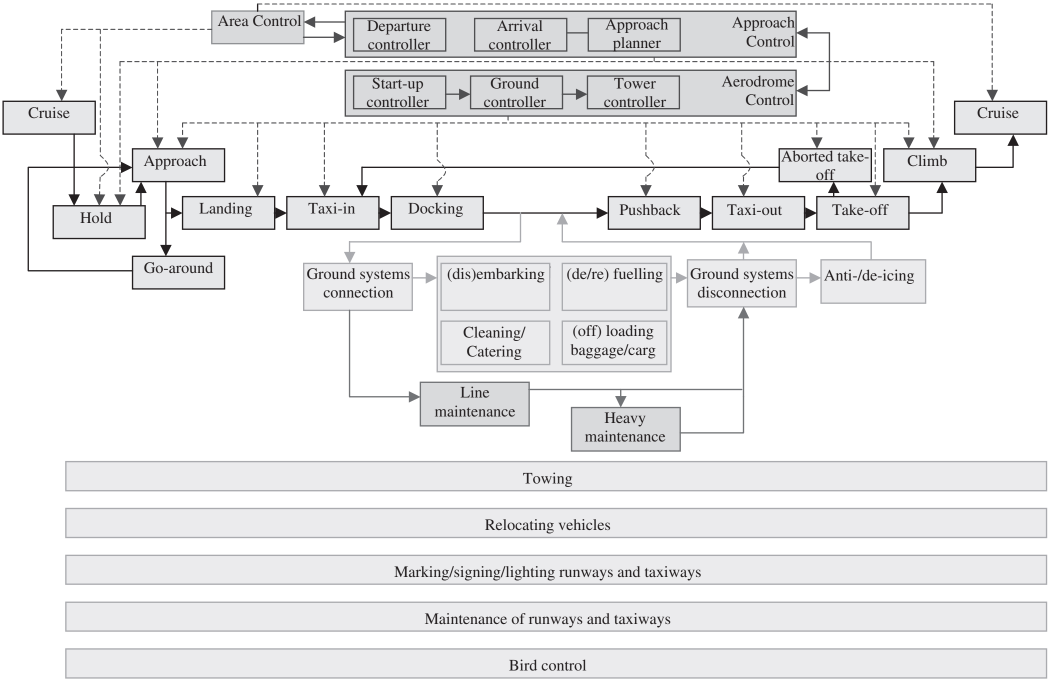

Figure 1. Gate to gate concept.

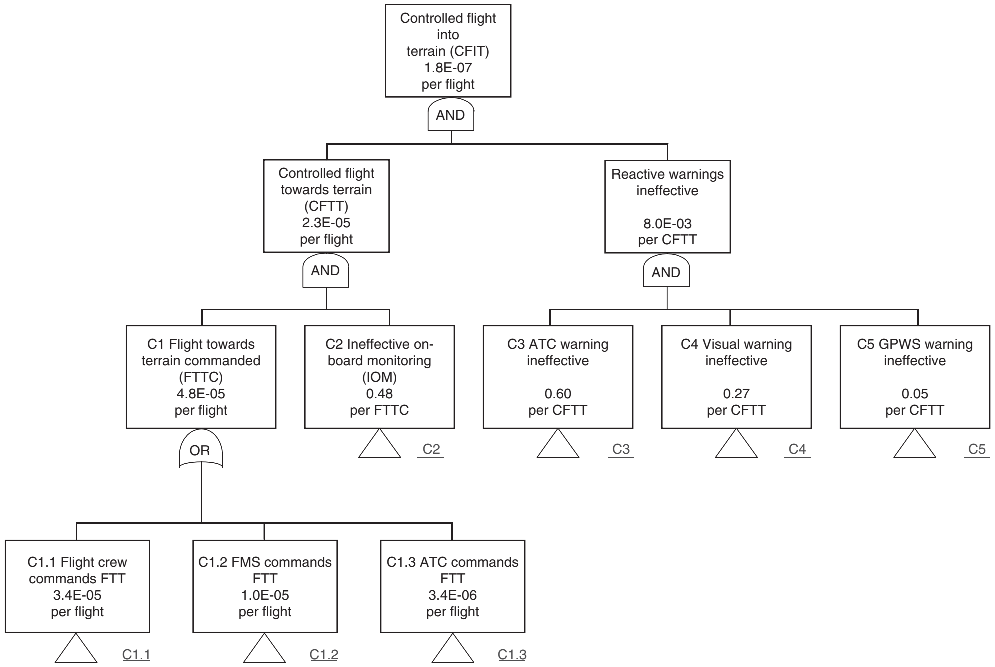
Controlled flight into terrain (CFIT) 1.8E-07 per flight
AND
Controlled flight towards terrain (CFTT) 2.3E-05 per flight
Reactive warnings ineffective 8.0E-03 per CFTT
AND
AND
C1 Flight towards terrain commanded (FTTC) 4.8E-05 per flight
C2 Ineffective on-board monitoring (IOM) 0.48 per FTTC
C3 ATC warning ineffective 0.60 per CFTT
C4 Visual warning ineffective 0.27 per CFTT
C5 GPWS warning ineffective 0.05 per CFTT
OR
C2
C3
C4
C5
C1.1 Flight crew commands FTT 3.4E-05 per flight
C1.2 FMS commands FTT 1.0E-05 per flight
C1.3 ATC commands FTT 3.4E-06 per flight
C1.1
C1.2
C1.3

Figure 2. Controlled flight into the ground. Partial fault tree.

through airspace all are considered as activities that are associated with this journey.

5.1 *Tree model*

One of the developments in the preparatory phase was tree-based and developed by DNV. Fault-trees and decision trees are well-established methodologies. They are extensively used in the analysis of nuclear power plants, electronic equipment, aircraft, aerospace and chemical installations [NASA 2003 NUREG, IEC611025, Dhillon 1992]. The technique can adequately describe probabilistic relationships and even the role of human behaviour in accident generation. It provides a rigorous technique to link causes and effects in a technological system. The generally accepted shortcomings of the fault-tree technique are that feedback loops cannot be described and that common mode or common cause failures are difficult to handle [NUREG]. The latter need extreme caution especially if the trees get complex. There is no limit to the complexity of the trees. A typical fault-tree for a nuclear power plant can have a many as 10.000 nodes [NRC 1975]. Trees are not restricted to known events. In fact many of the top-events have never occurred before but their feasibility is borne from properties of the system and systematic analysis of the potential effects of precursor events.

DNV worked out the example of controlled flight into the ground. A typical fault tree is depicted in Figure 2.

For the quantification of a fault-tree data are required for initiating or base events. These data have to be complete. Missing data can be obtained by expert judgement. For an absolute quantification these data have to be absolute. For comparison between systems or to determine the relative position of a system in a population of systems – for instance to decide whether a system is behaving better or worse than the population average – data are required for the system and for the population.

An especially difficult problem in this respect is the denominator problem. In many cases where data have been assembled, these pertain to the number of occurrences of certain faults or events. However population or exposure data are rarely available, such as the total number of events in which a certain fraction led to a fault. In the course of their involvement in the Schiphol case NLR has assembled a comprehensive database on airline accidents and incidents and it is expected that this will supply the necessary data [NLR 2004].

Management influences are always hard to quantify. It is difficult to establish an objective measure of quality for management systems. There are many assumptions but little proof about relationships between management quality and safety, especially if the quality is self-proclaimed and data in operational

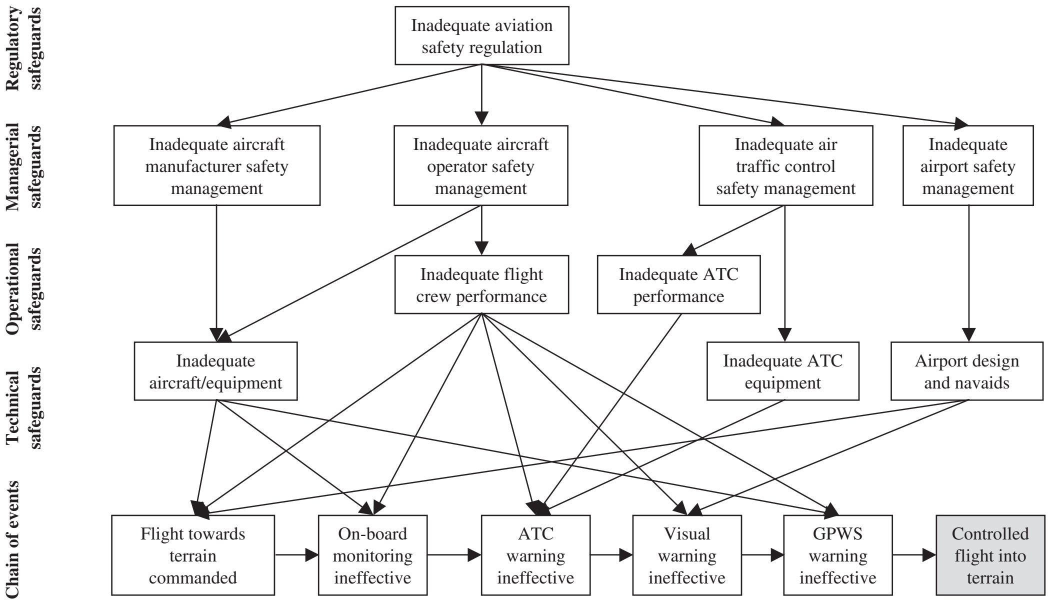
Regulatory safeguards
Managerial safeguards
Operational safeguards
Technical safeguards
Chain of events
Inadequate aviation safety regulation
Inadequate aircraft manufacturer safety management
Inadequate aircraft operator safety management
Inadequate air traffic control safety management
Inadequate airport safety management
Inadequate flight crew performance
Inadequate ATC performance
Inadequate aircraft/equipment
Inadequate ATC equipment
Airport design and navaids
Flight towards terrain commanded
On-board monitoring ineffective
ATC warning ineffective
Visual warning ineffective
GPWS warning ineffective
Controlled flight into terrain

Figure 3. Management influences in the DNV model.

terms with respect to the effect of management on the functioning of technical and operational systems is lacking [Bellamy et al 1999]. In the DNV model the influence of the various component of the management systems were accounted for by modifiers on the frequencies of the initiating events in the database (Figure 3), similar to the way it was done in the IRISK project [Papazoglou et al 1999].

5.2 *Belief net modelling*

One of the characteristics of a tree structure is that safety influencing factors that occur much earlier in the sequence of events (sometimes referred to as latent factors and often management/organisational in nature) are located deep in the tree structure [Reason 1990]. In practice, this means that in order to capture these factors the tree must be expanded enormously.

In addition these latent factors may influence many branches of the tree, which make them common mode factors. Hence the breakdown of the tree must stop at the level where these influences start. The elements at that level must be linked to the most important common modes through an interface to a Management Model, which is essentially a model of a different nature than a technical risk model. In searching for a modelling technique it is therefore important to assess how these problems can be resolved without losing essential influences and whilst keeping the tree manageable, but as complete as possible. A potential solution can be found from ongoing developments in the WORM project mentioned earlier [Ale et al 1998, Papazoglou et al 1999, Papazoglou et al 2003], in which the depth of the description of managerial influences is made dependent on the availability of data and the necessities arising from the fault-tree, event-tree and Bayesian Belief Net descriptions.

In the NLR model Bayesian Belief Nets are used as a modelling technique. Again pertinent statements are only possible on the base of data, which relate the output of a node, be it technical or managerial, to the inputs. These data can be qualitative or quantitative. If quantification of the probability of failure is required, obviously quantitative data are indispensable. As in the fault-tree method experts can estimate the probability and the mode of failure, if hard data are not available.

In the demonstration project, NLR + partners developed a general framework for the “technical model”. This consists of generic scenarios for departure from runway; undercarriage related events; general disintegration; loss of control; collision between aircraft; controlled flight into terrain. These generic accident scenarios have been fully quantified with real data and combined in a single model. “Missed approach” and “flight crew alertness” were developed to the level of detail that NLR thought was necessary for the complete model. The overall net-structure of the NLR model is given in Figure 4.

NLR used the well known management model based on the underlying management influences on safety critical tasks [Bellamy & Geyer 1991, Hurst et al 1991] and applied it to the aviation system.

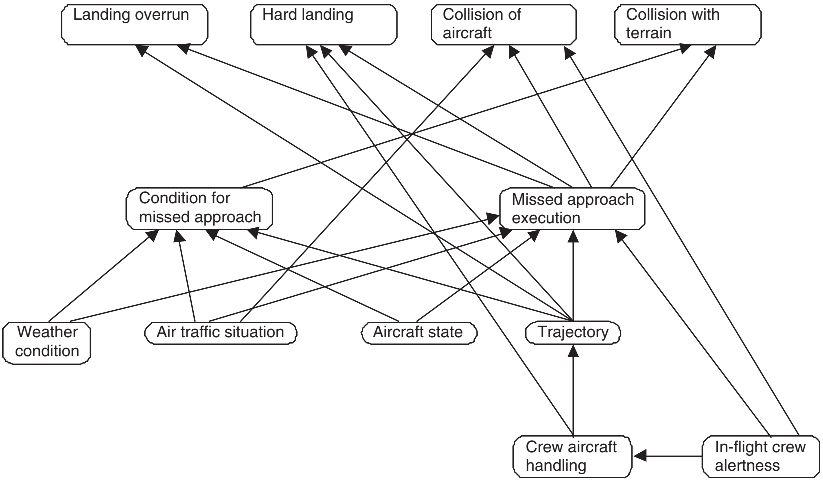

Figure 4. NLR Bayesian Belief Net structure for missed approach.

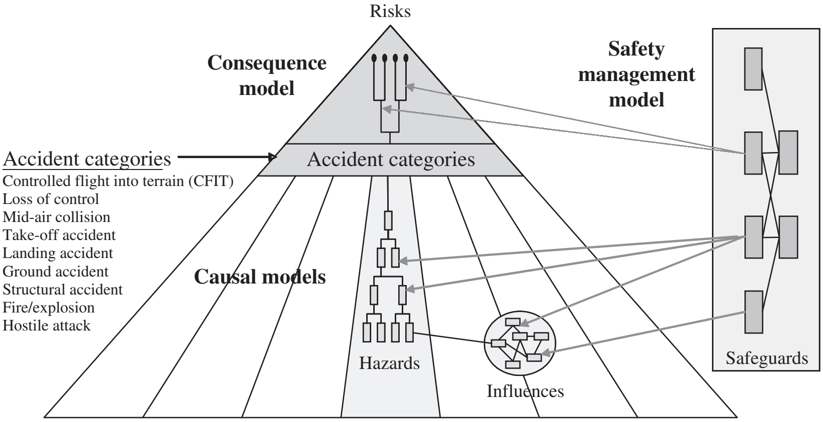

Figure 5. The model structure.

6 THE MODEL

Successful development of the causal model requires the integration of work by the research organisations, DNV, NLR and TU-Delft, and White Queen. The scope of work is based on an integration concept outlined below.

The approach is based on a conceptual overview of the model shown in figure 4. It is a true "causal risk model", since it covers consequences of accidents as well as their causes. As the consequences have been dealt with in the "statistical-causal" models that are used extensively for quantification of third party risk, there is no need for further analysis in this project. The majority of the modelling effort in this project focuses on the causes and on the coupling of the consequences to the decision-making.

Common elements in the causal models of different accident categories can be modelled separately by different members of the consortium. An example is flight crew fatigue, a demonstration subject in the NLR work, which may influence the causes of all accident categories. Figure 5 shows this common influence as a Bayesian network, feeding into a fault tree analysis of accident causes. In principle, either technique can be used as appropriate, depending on the nature of the hazards to be modelled.

The consequence model conventionally forms the right-hand side of a bow-tie model. This ensures that the outputs of the causal models (i.e. the frequencies of the different accident categories and their causal breakdowns) are combined in a consistent way to give the risk results, allowing valid comparison of options affecting different accident categories. The input requirements for the consequence models form the output specifications for the causal models. If followed, this will ensure that they are integrated as required.

The safety management model represents the elements of the safety management systems (aircraft operator, air traffic services, airports etc), which may influence many of the elements of the causal and consequence models. In simple terms, safety management controls the safeguards or barriers intended to prevent hazards leading to accidents. In the demonstration project DNV developed a simple audit-based approach for quantifying management influences, while NLR used the more elaborate modelling from the IRISK project. The latter modelling together with the interface between qualitative modelling and quantitative fault trees will be used to integrate management influence and technical failures [Mosleh et al 2004].

7 END POINTS

In the previous attempt the focus was on catastrophic events and more in particular the crash of an airliner into inhabited areas. This is a narrow scope and even a superficial analysis indicates that the efforts needed to make a full causal model for such crashes is hardly warranted if the only aim is to make it possible to allow more airport specific analysis than the current statistical approach already allows.

There are several reasons for this. The most important is that these crashes are rare events given the size of the population of aircraft and flights. Just as detailed causal modelling is not warranted for the estimation of the likelihood of aircraft catastrophic crashes, the crash incidents and their analysis are not sufficient to find systemic problems, solutions and improvements in a complex aeronautical system. For that to be possible, a larger range of accidents, incidents and near misses have to be taken into account.

8 CONCLUSIONS

The potential for development of a comprehensive causal model for aviation safety has been investigated in two pilot projects. These have indicated that the development of such a model is possible.

The influence of management on safety can be modelled by the management influence model developed in the IRISK project. The quantification can be handled by a previously developed interface.

The availability of data, which in many effort to quantify risks is a problem, may be solved by the availability of an extensive database on air traffic accidents and incidents.

REFERENCES

Ale, B.J.M., 1998, *The management of third party risk around a major airport*, in A. Mosleh and R.A. Bari (eds) Probablistic Safety Analysis and Management, Springer 1998

Ale, B.J.M. et al, 1998, *The Interface between the Technical and the Management Model for use in Quantified Risk Analysis* In: A. Mosleh and R.A. Bari (eds), Probabilistic Safety Assessment and Management, Springer, 1998

Ale, B.J.M. & Piers, M., 2000, *The Assessment and Management of Third Party Risk Around a Major Airport*, JhazMat, 71 (2000) 1–16

Amalberti, R. 2001. *The paradoxes of almost totally safe transport systems*, Safety Science, 37, 109–126

Bellamy, L.J. & Geyer T.A.W., 1991, *Pipework failure, failure causes and the management factor*, Management of in-service inspection of pressure systems, IMechE international conference, London, 12–13 March 1991

Bellamy, L. J. et al, 1999, *IRISK, development of an integrated technical and management risk control and monitoring methodology for managing on-site and off-site risks*, EC contract report ENV4-CT96-0243 (D612-D)

CAA Norway, 2004, *Final Report on the Risk Analysis in Support of Aerodrome Design Rules*

CAA Norway, NLA studies, 11th May 2004

Couwenberg, M.J.H., 1994, *Determination of the Statistical Accident Location Model From World-Wide Historical Accident Location Data*, National Aerospace Laboratory NLR, TR 94601 L

Cowell, P.G. et al, 2000, *A methodology for calculation individual risk due to aircraft accidents near airports*, National Air Traffic Services Ltd, R&D report 0007, London

Cowell, P.G. et al, 1997, *A Crash Location Model for use in the Vicinity of Airports*, NATS R&D report 9705, 1997

Dhillon, B.S., 1992, *Failure Mode and Effects Analysis-Bibliography*, Microelectronics and Reliability 32 (1992): 719–731

DNV, 2002, *Causal Modelling Of Air Safety*; Final Report, London, November 2002

FAA, 1998, Safer Skies Program

Federal Register: September 19, 2000 (Volume 65, Number 182) Rules and Regulations, Page 56617–56667

Gleave, D., 2002. *Basic Safety Philosophy, Aviation hazard Analysis, Operational Benefit Evaluation by Testing an A-SMGCS,* Contract 19990RD.10804 Deutsches Zentrum fur Luft und Raumfart, Braunschweig Germany

Gouweleeuw J.M., 1995, "*An Accident Location Model for Regional Airports*", National Aerospace Laboratory NLR, CR 95158 L

Hale, A., 2001, *Relating airport safety: the case of Schiphol,* Safety Science, Volume 37, Issues 2–3, March 2001, Pages 127–149

Hale, A., 2002. *Risk contours and risk management criteria for safety at major airports, with particular reference to the case of Schiphol,* Safety Science, Volume 40, Issues 1–4, February–June 2002, Pages 299–323

Hurst, N.W. et al, 1991, *A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies*, J. Haz. Mat., Vol. 26, no. 2, 1991, p.159–186, 1991

IEC611025 (faulttree electronic components)

Mosleh, A. et al, 2003, An Integrated Framework for Identification, Classification, and Assessment of Aviation Systems Hazards, Proceedings of PSAM7 (C. Spitzer, U. Smocker and V.N. Dang eds), ISBN 185233827X, Springer, 2004

NASA , 2003, *Columbia accident investigation board report*, August 2003

NLR, 2002, *Causal Modelling of Air Safety*, *a Demonstration Model* NLR CR 2002-662, NLR, Amsterdam, December 2002

NLR 2004, Externe Veiligheidsberekeningen in het kader van het Milieu Effect rapport “wijziging uitvoeringsbsluiten Schiphol”, NLR CR 2004-096, Amsterdam March 2004

NRC 1975 United States Nuclear Regulatory Commission, *Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants,* WASH-1400 (NUREG-75/014), Washington D.C., October 1975

NUREG, Fault tree handbook NUREG 01492

Papazoglou, I.A. et al, 1999, *Quantified Risk assessment of a chemical installation including management effects*, Risk and Crisis Management, University of Liege, Belgium, 5–7 May 1999

Papazoglou, I.A. et al, 2003, *I-Risk: development of an integrated technical and management risk methodology for chemical installations*, Journal of Loss Prevention in the Process Industries 16 (2003) 575–591

Piers, M.A. et al, 1993, *The Development of a Method for the Analysis of Societal and Individual Risk due to Aircraft Accidents in the Vicinity of Airports*, National Aerospace Laboratory NLR, CR 93372 L

Reason, J., 1990, *Human Error*, New York: Cambridge University Press

Reason, J., 1997, *Maintenance related errors: The biggest threat to aviation safety after gravity?* in “Aviation Safety”, H. Soekkha (ed.),VSP, Utrecht, The Netherlands, 1997

Roelen, A.L.C. et al, 2000, *Feasibility of the development of a causal model for the assessment of third party risk around airports*, Part 1: Main report, NLR-CR-2000-189-PT-1, NLR Amsterdam, April 2000

Smith, E., 1998, *Risks to Third Parties in the Vicinity of Airports – the Aircrash Program*, in A. Mosleh & R.A. Bari (eds), Probabilistic Safety Assessment and Management, Springer, September 1998

Technica, 1990, *Risk Analysis of Aircraft Impacts at Schiphol Airport*, 1884/EJS/ib, London.

Technica, 1991, Extension to Risk Analysis of Aircraft Impact at Schiphol Airport, C2475/EJS, London

TK 1996 , Tweede Kamer der Staten Generaal, zitting 1996–1997, TK 24804 nr 2

TK 2002, Tweede Kamer der Staten Generaal, zitting 2002–2003, TK 27603 nr 62 (“Motie van Gijzel”)

WORM 2003, *Workgroup Occupational Risk Model, (WORM), project description*, April 2003 Ref: 260403-1 Prepared for: Ministerie SZW Postbus 93356, 2509 AJ Den Haag