



DET NORSKE VERITAS

FAULT TREE MODELLING FOR THE  
CAUSAL MODEL OF AIR TRANSPORT SAFETY  
- FINAL REPORT

for

MINISTERIE VAN VERKEER EN WATERSTAAT

DNV PROJECT No. C21004587/3  
REVISION 0 20 JUNE 2008

PREPARED BY: JOHN SPOUGE

REVIEWED BY: GRAHAM VERNON

APPROVED BY: JOHN SPOUGE

DET NORSKE VERITAS LTD  
*DNV Industry*

Palace House  
3 Cathedral Street  
London SE1 9DE  
United Kingdom

Tel : + 44 (0) 20 7357 6080  
Fax : + 44 (0) 20 7716 6730  
<http://www.dnv.com>

Registered in England  
No.: 1503799

MANAGING RISK



## Management Summary

The Ministerie van Verkeer en Waterstaat (V&W) commissioned a Causal Model of Air Transport Safety (CATS) with the aim of providing a thorough understanding of the causal factors underlying the risks of air transport accidents, so that efforts to improve safety can be made as effective as possible.

The CATS model has been developed by a consortium including Delft University of Technology (TUD), Det Norske Veritas (DNV), National Aerospace Laboratory (NLR) and White Queen (WQ). The objective was to develop a full operational causal model, building on the experience gained in demonstration causal models developed by DNV and NLR during 2001-02. The present report summarises the contribution from DNV to the project up to completion of Phase 1 in 2008.

The CATS model uses a set of event sequence diagrams (ESDs) defining characteristic event sequences for each flight phase, each consisting of an initiating event and a sequence of pivotal events necessary for it to develop into an accident. The causes of each initiating event and pivotal event are demonstrated and quantified using fault tree (FT) models. To simplify development of these models, the ESDs have been grouped into broad accident types. The influences of flight crew, air traffic controller and maintenance performance are represented using Bayesian Belief Networks (BBNs), which also represent the common causes underlying the fault trees. The consequences of the events are modelled represented using probability-fatality (FN) curves and damage profiles. In order to combine the different models, they are all implemented in a giant BBN.

DNV's contribution to the consortium has included:

- Construction of fault tree models to quantify the causes of each initiating and pivotal event of each ESD.
- Definition of the effects of user inputs to represent specific cases in the fault tree.
- Definition of the uncertainty distributions for the fault tree base events, covering uncertainty in the average event probabilities and variability between different flights.
- Construction of a consequence model, providing fatal accident probabilities and frequency-fatality (FN) curves for each ESD.

The CATS model implements the fault trees and consequence model in a giant BBN. Inputs from users are represented as mappings conditioning the BBN, thus changing the probability distributions to represent specific operational cases or management interventions.

## Contents

1.	INTRODUCTION.....	1
1.1	Background.....	1
1.2	Objectives.....	1
1.3	General Approach.....	1
1.4	Report Structure.....	2
2.	FAULT TREE MODELLING.....	3
2.1	Requirement.....	3
2.2	ESD Structure.....	3
2.3	Fault Tree Grouping.....	4
2.4	Fault Tree Development.....	5
2.5	Case-Specific Modifications.....	8
2.6	Uncertainties.....	10
2.7	Variability.....	11
2.8	Dependencies.....	12
2.9	Validation.....	13
3.	CONTROLLED FLIGHT INTO TERRAIN.....	14
3.1	Definition and Importance.....	14
3.2	CFIT Scenario.....	14
3.3	Event Sequence Diagram.....	14
3.4	Barrier Model.....	15
3.5	CFIT Accident Frequency.....	17
3.6	Quantified ESD.....	17
3.7	Causal Data.....	18
3.8	CFIT Fault Tree.....	18
3.9	Uncertainties.....	20
3.10	Case-Specific Modifications.....	20
3.11	Validation.....	21
4.	LOSS OF CONTROL IN FLIGHT.....	22
4.1	Definition and Importance.....	22
4.2	LOCF Scenarios.....	22
4.3	Event Sequence Diagram.....	22
4.4	Barrier Model.....	23
4.5	Causes of Barrier Failure.....	24
4.6	LOCF Data.....	24
4.7	LOCF Fault Tree.....	25
4.8	Contributions.....	27
4.9	Case-Specific Modifications.....	28
4.10	Uncertainties.....	29
4.11	Validation.....	30
5.	LOSS OF CONTROL IN TAKE-OFF.....	31
5.1	Definition and Importance.....	31
5.2	LOCT Scenarios.....	31
5.3	Event Sequence Diagram.....	31
5.4	Barrier Model.....	32
5.5	LOCT Data.....	32
5.6	LOCT Fault Tree.....	32
5.7	Case-Specific Modifications.....	34

6.	LOSS OF CONTROL IN LANDING .....	35
6.1	Definition and Importance .....	35
6.2	LOCL Scenarios .....	35
6.3	Event Sequence Diagram .....	35
6.4	Barrier Model.....	36
6.5	LOCL Data .....	37
6.6	LOCL Fault Tree.....	37
6.7	Case-Specific Modifications .....	39
7.	ENGINE FAILURE IN FLIGHT .....	40
7.1	Definition and Importance .....	40
7.2	Event Sequence Diagram .....	40
7.3	Barrier Model.....	40
7.4	Engine Failure Data.....	41
7.5	Engine Failure Fault Tree.....	41
7.6	Case-Specific Modifications .....	42
8.	CONSEQUENCE MODELLING.....	43
8.1	Requirement.....	43
8.2	Consequence Types .....	43
8.3	Aircraft Damage Profile .....	43
8.4	Fatal Accident Probability.....	44
8.5	Fatal Accident Frequency.....	44
8.6	On-Board Fatality Profile.....	45
8.7	Consequence Factor Model .....	46
8.8	Overall Accident Costs .....	47
9.	REFERENCES.....	50
10.	ACRONYMS .....	51
APPENDIX I	MODIFICATION OF FAULT TREE IN RESPONSE TO USER INPUTS	

## 1. INTRODUCTION

### 1.1 Background

The Ministerie van Verkeer en Waterstaat (V&W) commissioned a Causal Model of Air Transport Safety (CATS). The model has been developed by a consortium including Delft University of Technology (TUD), Det Norske Veritas (DNV), National Aerospace Laboratory (NLR) and White Queen (WQ). The present report summarises the contribution from DNV to the project up to completion of Phase 1 in 2008.

### 1.2 Objectives

The motivation for the project is the need for a thorough understanding of the causal factors underlying the risks of air transport accidents, so that efforts to improve safety can be made as effective as possible.

The objective of the CATS project is to develop a full operational causal model, building on the experience gained in the demonstration causal models developed by DNV and a consortium led by NLR during 2001-02.

The objective of the causal model itself is to represent the causes of air transport accidents, and the safeguards that are in place to prevent them. This must be done in a way that facilitates its use for:

- Improving understanding of the causes of air transport accidents.
- Identifying areas where improvements could be made to the technical and managerial safeguards against accidents.
- Quantifying the risk implications of alternative technical and management changes, allowing evaluation of their cost-effectiveness.

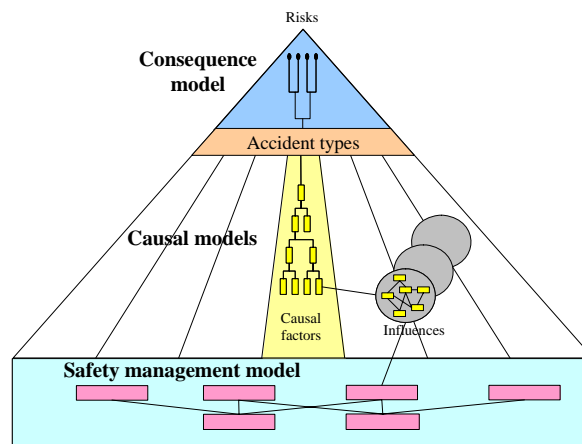
This requires a model of the causes of accidents, based on a realistic description of the air transport industry and its safety functions, including the relationship between technical and management systems.

### 1.3 General Approach

Aviation accidents tend to result from the combination of many different causal factors (human errors, technical failures, environmental and management influences) in certain characteristic accident categories (loss of control, collision, fire etc), whose causes and consequences differ according to the phase of flight in which they occur (taxi, take-off, en-route etc).

The CATS project approaches this complexity using a set of event sequence diagrams (ESDs) defining characteristic event sequences for each flight phase, each consisting of an initiating event and a sequence of pivotal events necessary for it to develop into an accident. The causes of each initiating event and pivotal event are demonstrated and quantified using fault tree (FT) models. To simplify development of these models, the ESDs have been grouped into broad accident types. The influences of flight crew, air traffic controller and maintenance performance are represented using Bayesian Belief Networks (BBNs), which also represent the common causes underlying the fault trees. The consequences of the events are modelled represented using probability-fatality (FN) curves and damage profiles. In order to combine the different models, they are all implemented in a giant BBN.

**Figure 1.1 Overall Causal Model Structure**



DNV's contribution to the consortium has included:

- Construction of fault tree models to quantify the causes of each initiating and pivotal event of each ESD.
- Definition of the effects of user inputs to represent specific cases in the fault tree.
- Definition of the uncertainty distributions for the fault tree base events, covering uncertainty in the average event probabilities and variability between different flights.
- Construction of a consequence model, providing fatal accident probabilities and FN curves for each ESD.

The CATS model implements the fault trees and consequence model in a giant BBN. Inputs from users are represented as mappings conditioning the BBN, thus changing the probability distributions to represent specific operational cases or management interventions.

#### **1.4 Report Structure**

This report outlines the general approach to the fault tree modelling (Section 2). Example sections of fault trees are given in the Sections 3-7. The report also summarises the consequence modelling that has been used to combine the different ESDs (Section 8). More comprehensive documentation is provided in separate reports [2-10].

## 2. FAULT TREE MODELLING

### 2.1 Requirement

The CATS model requires fault trees to quantify the causes of each initiating event and pivotal event in each of the set of ESDs. The probabilities of the fault tree top events should match the probabilities of the ESD events [1]. The fault trees should show the breakdowns of causes of these events, to the extent that is possible within the limitations of fault tree modelling. Where the causes result from human behaviour, the base events of the fault trees should link to the BBNs of human performance. Other base events of the fault trees should link to the user inputs of the CATS model. In order to integrate with the BBNs of human behaviour, the fault tree models are intended to be implemented in a giant BBN. To achieve this, the uncertainties in the base events must be described by probability distributions. The fault trees should be sufficiently detailed and sufficiently robust to contribute towards the objectives of the overall model.

### 2.2 ESD Structure

The CATS model uses a set of event sequence diagrams (ESDs) defining characteristic event sequences for each flight phase, each consisting of an initiating event and a sequence of pivotal events necessary for it to develop into an accident. The ESDs have been defined by NLR [1], and their initiating events are given in Table 2.1. There are in total 33 ESDs requiring fault trees.

**Table 2.1 List of ESDs**

ESD	Initiating event	Flight phases	FT group
1	Aircraft system failure	TO	LOCT
2	ATC event	TO	Collision
3	Aircraft handling by flight crew inappropriate	TO	LOCT
4	Aircraft directional control related systems failure	TO	LOCT
5	Operation of aircraft systems by flight crew inappropriate	TO	LOCT
6	Aircraft takes off with contaminated wing	TO	LOCT
7	Aircraft weight and balance outside limits	TO	LOCT
8	Aircraft encounters windshear after rotation	TO	LOCT
9	Single engine failure	TO	LOCT
10	Pitch control problem	TO	LOCT
11	Fire on board aircraft	CL, ER, AL	Fire/exp
12	Flight crew member spatially disorientated	CL, ER, AL	LOCF
13	Flight control system failure	CL, ER, AL	LOCF
14	Flight crew incapacitation	TO, CL, ER, AL	LOCF
15	Anti-ice system not operating	CL, ER, AL	LOCF
16	Flight instrument failure	CL, ER, AL	LOCF
17	Aircraft encounters adverse weather	CL, ER, AL	Structural
18	Single engine failure	CL, ER, AL	Engine
19	Unstable approach	AL	LOCL
20	Deleted (incorporated in ESD 19)	-	-
21	Aircraft weight and balance outside limits	AL	LOCL
22	Deleted	-	-
23	Aircraft encounters windshear during approach/landing	AL	LOCL
24	Deleted (incorporated in ESD 19)	-	-
25	Aircraft handling by flight crew during flare inappropriate	AL	LOCL

ESD	Initiating event	Flight phases	FT group
26	Aircraft handling by flight crew during roll inappropriate	AL	LOCL
27	Aircraft direction control related systems failure	AL	LOCL
28	Single engine failure	AL	LOCL
29	Thrust reverser failure	AL	LOCL
30	Aircraft encounters unexpected wind	AL	LOCL
31	Aircraft are positioned on collision course	CL, ER, AL	Collision
32	Incorrect presence of aircraft/vehicle on runway in use	TA, TO, AL	Collision
33	Cracks in aircraft pressure cabin	CL, ER, AL	Structural
34	Deleted (incorporated in ESD 17)	-	-
35	Flight crew decision error/operation of equipment error	CL, ER, AL	CFIT
36	Ground collision imminent	TA	Collision
37	Wake vortex encounter	CL, ER, AL	LOCF

Several of the ESDs apply in more than one flight phase. The flight phase codes shown in the table are:

- TA - taxi
- TO - take-off
- CL - climb
- ER - en-route
- AL - approach & landing

### 2.3 Fault Tree Grouping

For developing and documenting the fault tree models, DNV has grouped the ESDs into 8 accident types:

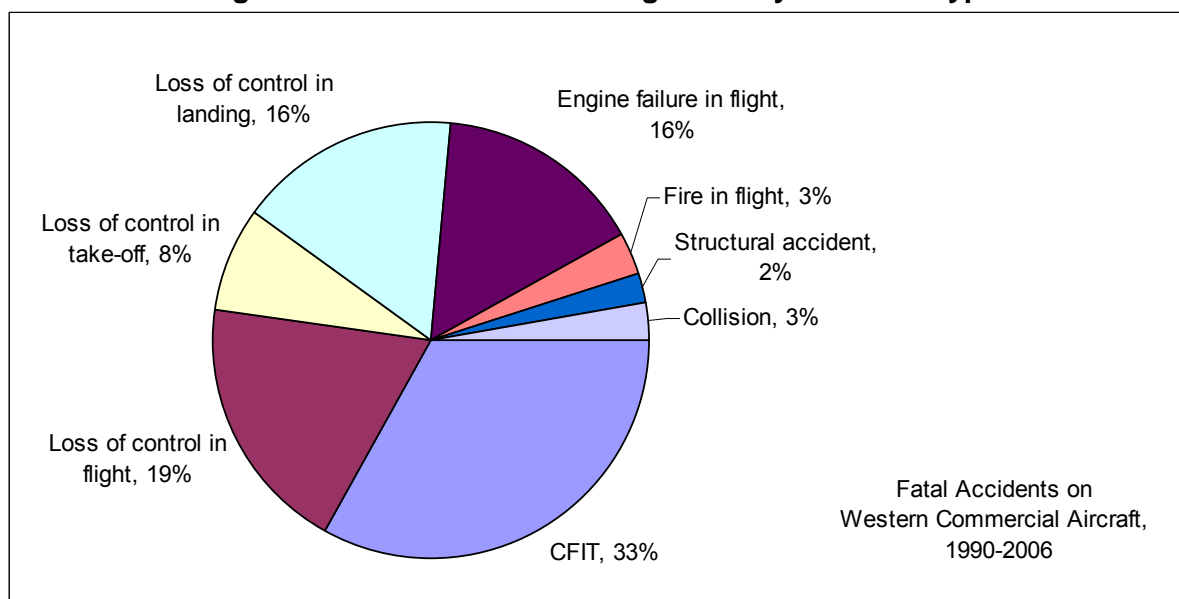
- Controlled flight into terrain (CFIT)
- Loss of control in flight (LOCF)
- Loss of control in take-off (LOCT)
- Loss of control in landing (LOCL)
- Engine failure in flight
- Structural failure in flight
- Collision (including mid-air, runway and ground collision)
- Fire/explosion

These fault tree groups are also shown in the table above.

Examples of the fault tree models are given in the following sections, together with selected details on how they were developed and validated. Full details are provided in the reports on each accident type [2-9].

A rough indication of the relative importance of these accident types is obtained from an analysis of the ADREP database. Fatal accidents on Western commercial aircraft of 5700 kg mean take-off weight (MTOW) or more during 1990-2006 have been categorised into the above accident types. The results are shown in Figure 2.1. Personal and security accidents, and other accidents that cannot be categorised into the above types have been excluded.

**Figure 2.1 Fatal Accidents Categorised by Accident Type**



## 2.4 Fault Tree Development

### 2.4.1 Barrier Model

Each fault tree is based on an event scenario (ESD), which represents a group of events with significant causal similarity. The ESD consists of an initiating event, followed by possible sequences of pivotal events, leading towards possible end events, at least one of which is an accident state. Quantified ESDs, showing the probabilities of each initiating, pivotal and end event, have been supplied for the project by NLR [1].

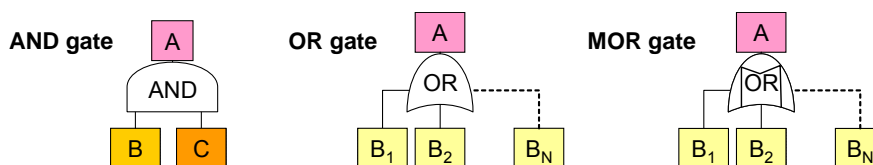
Each fault tree is based on a barrier model of the scenario. The barriers are managed safeguards or logical circumstances that should in most cases prevent the accident from occurring. The reasons for failure of each barrier are therefore the causes of the accident, and are represented in the fault tree. The possible failure causes are identified from accident and incident experience, together with logical identification of possible events that have not occurred.

The barrier model directs attention towards possible interventions to reduce the likelihood of the accident. Each cause is also an opportunity for an intervention to make it less likely. It should also be noted that interventions could aim to add further barriers, or reduce dependencies that might undermine the effectiveness of the barriers.

### 2.4.2 Logic Gates

The fault trees provide a logical structure showing how causal factors could combine to cause an initiating or pivotal event of the ESD. The ESD shows how combinations of these events may cause an accident. Figure 2.2 shows the different types of logic gates used in the fault tree. They are explained in turn below.

**Figure 2.2 Schematic Fault Tree Logic Gates**



AND gates are used where an event A has two independent, necessary causes B and C. The probability is:

$$P(A) = P(B) \times P(C) \text{Fout! Bladwijzer niet gedefinieerd.}$$

OR gates are used where an event A may result from N alternative causes  $B_i$ . Assuming the causes are independent, the probability is:

$$P(A) = 1 - \prod_{i=1}^N (1 - P(B_i))$$

MOR gates are used where an event A may result from N alternative causes  $B_i$  that are mutually exclusive (i.e. only one can occur at once by definition). The probability is:

$$P(A) = \sum_{i=1}^N P(B_i)$$

In developing the fault tree, a top-down approach is followed, which reverses these calculations. The top events of the fault trees are known from the initiating and pivotal events from the ESD. These are split into events corresponding to unsuccessful performance of each barrier. At each AND gate, additional probability data or assumptions are needed to quantify the input events. These unsuccessful barrier events are then further split into the causes of barrier failure. At each OR gate, causal distributions are needed as described below.

Development of the fault tree model has followed the same approach as used by the EUROCONTROL Integrated Risk Picture (IRP) [11]. By agreement with EUROCONTROL, the IRP models for collisions have been adopted from this source. Some changes have been necessary because the explicit modelling of common-cause events in the IRP is not required in CATS, since this aspect is represented by BBNs.

### 2.4.3 Causal Data

Quantification of the fault tree model uses distributions of causes obtained from accident and incident experience. The quality of information in ADREP about accident causes is not sufficient to support the present analysis. Therefore original accident investigation reports have been used where available. In other cases, the summary information from Airclaims, Aviation Safety Network, Flight Safety Foundation and others explains the causes in sufficient detail to relate to the barrier model. Incident reports have also been used where available. The term “event” is used below to refer to both accident and incidents.

To quantify the fault tree, it is not necessary to know the causes of every event that has occurred. Since the ESDs have been quantified using probability data, consisting of comprehensive counts of the numbers of events among known flight exposure, the causal breakdown in the fault trees can be quantified from a representative sample of events. It is

therefore assumed that the events whose causes are known, and which are used to quantify the causal breakdowns in the fault trees, are representative of the causes of the full set of accidents.

For ESDs with little or no accident experience, the fault trees are quantified using experience from precursor incidents. These are incidents that were prevented from developing into the relevant accident by the success of one or more barriers. It is assumed that the causes of these incidents indicate the likely causes of initiating events in future accidents. The causes of the necessary further barrier failures can be obtained from other ESDs in which the same barriers are relevant, or as a last resort from expert judgement about their relative likelihood. In general, the fault trees have been developed only to a level that can be quantified mainly from available accident or incident data, and pure judgements about event probabilities have been minimised.

#### 2.4.4 Event Contributions

The fault tree model shows the “contribution” of each causal factor, which gives a simple indication of its relative importance to the accident frequency for that ESD. The contribution is calculated following a top-down approach, beginning from the top event for each pivotal event of the ESD, which is given a contribution of 1.

At an AND gate, the contribution of input events B and C is taken to be the same as the output event A (see Figure 2.2). This is the same as in the Fussell-Vesely importance measure, reflecting the fact that the output changes in direct proportion to changes in either input.

At an OR gate, the contribution of the output event A is partitioned among the input events  $B_i$  as follows:

$$C(B_i) = \frac{C(A) \times P(B_i)}{\sum_{j=1}^N P(B_j)}$$

where:

$C(B_i)$	=	contribution of input event $B_i$
$C(A)$	=	contribution of output event A
$P(B_i)$	=	probability of input event $B_i$

This is the Differential Importance Measure [12] based on a uniform change for all inputs, and has the property of being additive within each OR gate, i.e.:

$$C(A) = \sum_{i=1}^N C(B_i)$$

The contribution gives a simple estimate of the maximum benefit, expressed as a fraction of the accident frequency, which could be achieved by improvements in each specific factor. A contribution of 1 implies that the risk would be eliminated if the causal factor could be prevented. Smaller contributions imply proportionately smaller effects. However, due to the non-linearity of fault tree (notably the large probabilities), any such single measure of causal contribution is only an approximation. More accurate results could be obtained where necessary through comprehensive sensitivity testing, which is appropriate as part of the giant BBN model.

## 2.5 Case-Specific Modifications

The fault tree model represents a generic average of commercial aircraft operations. It is based on causal breakdowns drawn mainly from experience during the period 1990-2006, which provides sufficient accidents and incidents to quantify the model while also being reasonably consistent with modern operational practice. It is consistent with the data choices that were made in quantifying the ESDs. In particular, the ESD for CFIT represents only aircraft with a terrain awareness and warning system (TAWS), since this has been required for commercial aircraft since 2007. In other respects, the fault tree model represents an average of commercial experience during earlier periods, and is assumed to be applicable to current operations.

The fault tree model is able to represent specific cases that differ from the generic average. These cases are defined by user inputs, which select from the possible states of various influences on the base events of the fault tree. Ideally these should be continuous variables, but in practice suitable metrics and data are usually not available. Therefore most of the influences are defined as sets of discrete states. Each state has an exposure probability, defined as the proportion of world-wide flights of commercial aircraft that experience the influence in that state. The generic case represented in the fault tree is the average of these specific states.

The relationship (or mapping) between an influence and a fault tree base event is expressed as a modification factor (MF), defined as:

$$MF = \frac{\text{Base event probability in specific state}}{\text{Base event probability in generic case}}$$

The effects of these mappings on the overall risks are expressed as risk ratios (RR), defined as:

$$RR = \frac{\text{Accident frequency in specific state}}{\text{Accident frequency in generic case}}$$

MF and RR represent model inputs and outputs respectively. The difference between them arises from the non-linearity of the fault tree model.

When quantifying the MFs, the following types of influences are distinguished:

- Deterministic influences. These are where the fault tree event is defined so that it can only occur in one of two possible input states (e.g. wind-shear present or absent), so that the MF is determined directly by the exposure probability of the chosen state.
- Data-based influences, i.e. probabilistic influences quantified using stratified data. These are where the fault tree event may occur in *any* of a set of alternative states (e.g. aircraft generation 1, 2, 3 or 4), whose probabilities of occurrence and MFs can be obtained using accident and exposure data.
- Judged influences, i.e. probabilistic influences quantified using judgement. These are where the fault tree event may occur in *any* of a set of alternative states, whose relative probabilities are based on judgement in the absence of any useful data.

- Functional influences i.e. probabilistic influences expressed as an analytical function of a user input (e.g. airport elevation). The function may be a judgement that the fault tree event is proportional to the input, or it may be a fit to data-based influences.

Table 2.2 lists the influences that are represented in the fault tree model. They are explained in more detail in Appendix I.

**Table 2.2 List of Fault Tree Influences**

GROUP	INFLUENCE	STATES/METRIC	TYPE
Operating environment	Geographical region	ICAO regions	Data
	National income	GDP \$/capita	Data
	Traffic level	Fraction of 1990-2005 average	Function
	TMA complexity	ATC vectoring commands per flight	Function
Flight operation	Flight phase	Taxi, take-off, climb, en-route, approach/landing	Data
	Operation type	Passenger, cargo, non-revenue	Data
Aircraft	Aircraft type	Large jet, turboprop, small jet	Data
	Aircraft size	kg MTOW	Data
	Aircraft generation	1, 2, 3, 4	Data
	GPWS type	None, early, standard, TAWS	Data
	ACAS	Installed, not installed	Deterministic
	PWS	Installed, not installed	Deterministic
	Autoflight use	Fraction of trajectory changes via FMS	Function
Airport	Airport elevation	ft above mean sea level	Function
	Approach type	Precision, non-precision	Data
	Runway length	Short, medium, long	Judged
	Runway crossing	Runway crossings per flight	Function
	Runway condition	Wet, dry	Judged
	Runway slipperiness measurement	Frequency	Judged
	Runway slipperiness criteria	Used, not used	Judged
	Runway maintenance criteria	Used, not used	Judged
	FOD criteria	Used, not used	Judged
	Bird management	Used, not used	Judged
ANSP	LLWAS	Installed, not installed	Deterministic
	STCA	Installed, not installed	Deterministic
	Ground radar	Installed, not installed	Deterministic
	RIMCAS	Installed, not installed	Deterministic
	Terminal area radar	Installed, not installed	Deterministic
	MSAW	Installed, not installed	Deterministic
Ambient environment	Light condition	Daylight, dark	Judged
	Visibility at airport	Restricted, unrestricted	Judged
	Visibility in flight	IMC, VMC	Judged
	Cross-wind	Strong, weak	Deterministic
	Wind-shear	Present, absent	Deterministic
	Turbulence	Strong, weak	Deterministic
	Icing at airport	Freezing, above freezing	Deterministic
	Precipitation at airport	None, light, moderate, heavy	Data

At present, each of these influences is considered as if its effects were independent of all other influences. In reality, many of the influences are correlated. In principle, these correlations could be modelled using BBNs, but developing suitable models is challenging,

and will be considered in future work. Meanwhile, it must be recognised that combination of the MFs from different influences may be unrealistic, and may tend to over-estimate the effects (i.e. produce risk ratios that diverge excessively from 1).

Other influences (notably the standard of performance of flight crew, ATC and maintenance personnel) are represented in human performance BBNs elsewhere in the CATS model. The influences of these parameters are represented by conditioning the BBN to particular values within the distributions. Their effect on the fault tree is assumed to be the same for each base event that has a logical connection to the human performance. This is a simplification, which might be improved in future work.

## 2.6 Uncertainties

The fault trees present best-estimates of the average probabilities of events among commercial flights world-wide. The following types of uncertainty can be distinguished in the results:

- Variability (also known as aleatory or Type A uncertainty). This is due to natural randomness. Due to many influences, some flights experience a higher probability of accidents than others.
- Epistemic uncertainty (also known as Type B uncertainty). This is due to lack of knowledge. It is impossible to know exactly what the probability of an event is, although this uncertainty can be reduced by more data collection or better modelling. Epistemic uncertainties include:
  - Model uncertainty (also known as structural uncertainty). This is due to simplifications or lack of realism in the formulation of the model. This is very difficult to quantify, unless by comparing independently produced models.
  - Sampling uncertainty (also known as parametric uncertainty). This includes uncertainties due to:
    - Data quantity. This arises from the fact that relatively small datasets are available (and sometimes no accident experience at all). Standard mathematical techniques are available to quantify this type of uncertainty.
    - Data representativeness (or bias). This arises if the selected data does not match the problem of interest, e.g. it may be old or based on a few countries that investigate accidents thoroughly. Once these biases are understood, corrections can be made to minimise their effects.
    - Data interpretation. This arises because the accidents and incidents may be not fully understood or not clearly linked to the model. This is again very difficult to quantify, unless by independent evaluations of the available data.

In order to convert the fault trees into BBNs, it is necessary to define the complete uncertainty distribution (including variability) for each base event. This is expressed as the probability distribution for MF, as defined above, which has a mean value of 1 by definition.

Comprehensive analysis of all sources of epistemic uncertainty would be resource intensive and itself extremely uncertain. In order to obtain probability distributions for the fault tree base events, a simplified approach is adopted, choosing the largest confidence range from the following sources:

- If the event probability is based on data, the distribution is calculated directly from the data quantity. On-demand probabilities are represented by a Beta distribution; per-flight frequencies are represented by a chi-square distribution.
- If estimates of the probabilities are available from alternative sources or using alternative judgements, the largest and smallest of these alternatives are used to define the extremes of a triangular distribution, with the best-estimate (i.e. MF=1) used as the modal value.
- In the absence of any data or alternative approaches, the uncertainty range is defined by judgement. The distribution is assumed to be lognormal if the log uncertainty range is symmetric, or triangular otherwise.

The chosen epistemic uncertainty distribution is combined with the variability distribution (Section 2.7), to obtain the complete uncertainty distribution for each base event.

## 2.7 Variability

The probability distribution of variability is quantified by combining the influences in Table 2.2 above for each base event, assuming they are independent. If there are  $M$  influences, and the  $j$ 'th influence has  $S_j$  possible states, the total number of possible combinations of influence states is:

$$S_{total} = \prod_{j=1}^M S_j$$

If the influences are all independent, the overall MF of any particular combination for a given base event  $B_i$  is the product of the independent MFs:

$$MF_{i,z} = \prod_{j=1}^M MF_{i,j,k}$$

where:

$$\begin{aligned} MF_{i,z} &= \text{MF for } B_i \text{ in influence combination } z \text{ (which ranges from 1 to } S_{total}) \\ MF_{i,j,k} &= \text{MF for } B_i \text{ in state } k \text{ (which ranges from 1 to } S_j) \text{ of influence } j \text{ (which} \\ &\text{ ranges from 1 to } M) \end{aligned}$$

The index  $z$  is used to represent the influence combination ( $j, k$ ). There must be a consistent mapping between ( $j, k$ ) and  $z$ .

The probability of this combination is:

$$p(MF_{i,z}) = \prod_{j=1}^M p(E_{j,k})$$

where:

$$p(MF_{i,z}) = \text{probability of occurrence of influence combination } z$$

$p(E_{j,k}) =$  probability of occurrence of state k of influence j among exposure E

This gives a set of pairs of modification factors and probabilities  $\{MF_{i,z}, p(MF_{i,z})\}$ . To extract the percentiles of this distribution, the set is sorted into MF order and the cumulative probabilities extracted:

$$P(MF_i) = \sum_{z=1}^{S_{total}} p(MF_{i,z}) \mid MF_{i,z} \leq MF_i$$

The percentiles can be found from this distribution. The sum of probabilities must be 1 and the expectation of the MF distribution should also be close to 1 as required.

In practice, these distributions are highly skewed (e.g. Figure 4.7). This is because most influences consist of rare adverse influences and more common beneficial ones. For example, most flights are in new aircraft, Western countries, dry weather etc. Because variability is defined relative to the average, these cases produce MFs only slightly below 1. The rarer cases of old aircraft, non-Western countries, wet weather etc produce much higher MFs (especially when combined under the assumption of independence) with low probabilities.

## 2.8 Dependencies

Dependent events are defined [13] as pairs of events A and B, where the combined probability  $P(A \text{ and } B) \neq P(A) P(B)$ . This may be because the events are functionally linked, or because they are associated through some extrinsic influence such as human interaction or the environment.

Dependencies are important for systems with multiple barriers such as aviation, because the overall accident probability may be very sensitive to the degree of dependency between the barriers. If this is inadequately represented in the model, substantial errors may occur in the results. The top-down approach to quantification used in the CATS fault trees ensures that the overall probabilities are consistent with actual accident data, but the effects of dependencies could in principle lead to errors in the predicted effects of interventions.

In general, fault tree models attempt to represent functional dependencies, to the maximum practical extent, in order to obtain base events that are as independent as possible. Common cause failures (CCFs) represent the residual dependencies between base events that are not explicitly modelled in the fault tree structure. This approach is used in EUROCONTROL's IRP.

In the CATS model, the BBNs of human behaviour represent the main dependencies between base events. The implementation of the fault trees in the giant BBN takes account of the majority of these dependencies without requiring an additional CCF model. It is acknowledged that some errors remain, which could only be eliminated through a full probabilistic model, which would require substantial additional data and elicitation of correlations.

Another type of dependency occurs when an aircraft enters an ESD in a degraded state following a non-catastrophic event in a previous ESD. This linkage between ESDs is not modelled at present.

## 2.9 Validation

The fault tree model has been implemented for this project in a spreadsheet. Compared to an existing fault tree program, spreadsheet implementation has the advantage of flexibility (especially in performing both top-down and bottom-up calculations), but it requires more careful validation.

One key requirement is to verify that the fault tree has been constructed correctly. The first line of defence against errors in fault tree construction is DNV's quality assurance (QA) system. This requires:

- Definition of responsibility for each part of the work. This is defined in the report on each accident type [2-9] and in the documentation within the fault tree package, which is to be included in CATSPAWS.
- Detailed self-checks by the responsible person at each stage of the work. This is an essential part of DNV's competence training for risk analysts. Some of the available checks are explained below.
- Independent review of each part of the work. The extent of this review depends on the competence of the responsible person, as judged from previous reviews. The identity of the reviewer is documented in the report on each accident category.
- Full documentation of the work through project reports. The project reports provide detailed documentation, which complements the summaries in the fault tree package and CATSPAWS.

No QA system can guarantee that there are no errors in a model as complex as the CATS fault trees. Nevertheless, a high degree of error correction is achieved, through use of the following self-checks:

- Each fault tree model is implemented in a gate-by-gate form, showing all intermediate results, which are also included in the project reports. This allows manual checks of each stage in the model, and this has been effective in identifying errors in the model.
- Each fault tree model is implemented twice, quantified once from the top down (developing base event probabilities), and once from the bottom up (recalculating the top event probabilities). The fact that this returns numerically identical probabilities helps trap a high proportion of errors in model construction.
- The contributions of causal factors for each barrier in the fault tree sum to 1, due to the use of the metric non-dimensional risk reduction worth. This allows a simple check against numerical errors in quantification of these results. The relative importance of each cause of barrier failure also allows a check against input data and subjective expectation.
- The fault trees have been implemented independently as BBNs, which provides a further verification that the calculations are consistent with the chosen logic gates.

In addition to checks of the fault trees themselves, there has been some cross-checking of the top event probabilities against the corresponding events in the ESDs, in the cases where the fault trees and ESDs were quantified independently. Quantification of epistemic uncertainty has also motivated consideration of alternative sources of probability estimates, which is believed to increase the quality of the result.

### 3. CONTROLLED FLIGHT INTO TERRAIN

#### 3.1 Definition and Importance

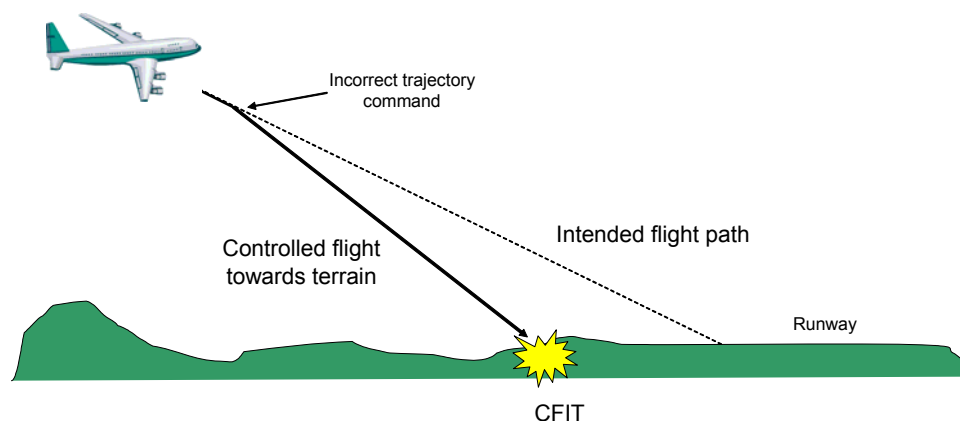
Controlled flight into terrain (CFIT) is defined as an accidental in-flight collision with terrain, water or obstacle without prior loss of control. It includes accidental collisions with buildings, towers etc, provided that the aircraft is under control until the collision occurs. Accidents where the point of impact is less than 500m before the runway threshold are covered under landing accidents (Section 5). Accidents where the flight crew incorrectly believe the aircraft is out of control are covered under loss of control in flight (Section 4).

CFIT is one of the main causes of fatal accidents in commercial aviation. Among world-wide operations of Western commercial aircraft during 1990-2006, CFIT accounted for 33% of fatal accidents (Figure 2.1) and virtually the same proportion of fatalities.

#### 3.2 CFIT Scenario

Although CFIT accidents can arise in different ways, there are sufficient common features to define a characteristic scenario (Figure 3.1), which is represented in the fault tree model. The most obvious common feature is a deviation from the intended flight path, consisting of a controlled flight towards terrain, during which time various warnings may be received. If these are not successful, a CFIT will result.

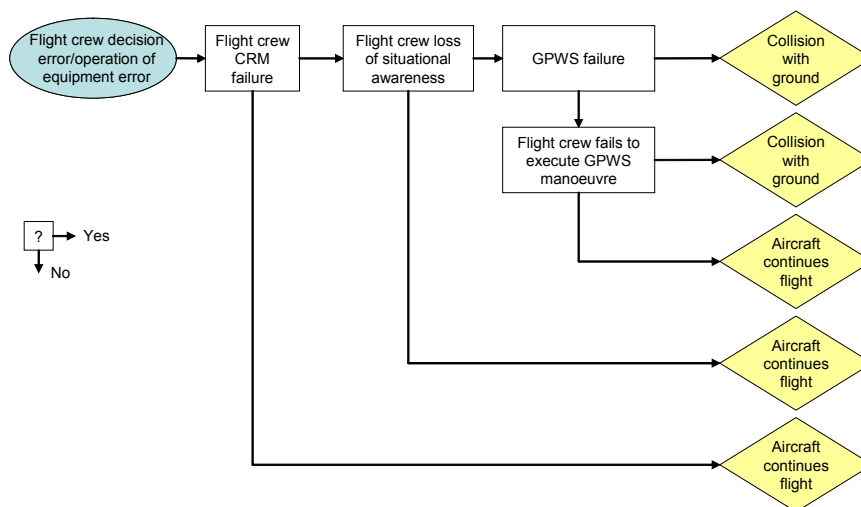
Figure 3.1 Simplified CFIT Scenario



#### 3.3 Event Sequence Diagram

A single event sequence diagram (ESD 35) has been specified by NLR [1] to represent the CFIT accident category. This is shown in Figure 3.2. The fault tree is required to give the causal breakdown for each initiating and pivotal event for each flight phase. Dependencies between the events will be represented by the BBN model of flight crew performance.

**Figure 3.2 CFIT Event Sequence Diagram**



### 3.4 Barrier Model

The following are the major barriers against CFIT accidents, all of which must be unsuccessful if the accident is to occur. They are fully described and reported in EUROCONTROL's IRP [11]:

- Trajectory command procedures. The trajectory of an aircraft refers to its course and rate of climb/descent. Trajectory commands may be made by the flight crew, the flight management system (FMS) or air traffic control (ATC) instructing the flight crew. In each case, flight procedures, ATC procedures and the FMS design are in part intended to ensure that the trajectory commands do not bring the aircraft into conflict with terrain.
- On-board monitoring. The pilot not flying (PNF) should monitor the actions of the pilot flying (PF) and cross-check key inputs using duplicate instrumentation. In addition, the pilots should monitor the FMS, and should also review instructions from ATC before implementing them. This monitoring may detect and correct incorrect trajectory commands before the aircraft departs from the intended flight path.
- ATC warning. Monitoring of the aircraft's position by ATC may allow a warning of terrain conflict. Major airports have terminal area radar (TAR) that provides ATC with information about aircraft location and altitude. Some ATC units have a minimum safe altitude warning (MSAW), which provides an acoustic and visual alert to the controller if the aircraft descends below the applicable minimum safe altitude. In the absence of TAR, ATC monitoring depends on radio position reports by the aircraft. In either case, the controller must pass the warning to the flight crew via radio.
- Visual warning. In visual meteorological conditions (VMC), the flight crew may supplement flight instruments with observation of the ground, which may in some cases give warning of terrain conflict. During approach to landing, if the terrain is not in sight at a pre-determined decision height, the flight crew should follow a missed approach procedure. This is also considered a type of visual warning, although it is triggered by an absence of visual contact.

- GPWS warning. The ground proximity warning system (GPWS) provides last-minute warning of terrain conflict. A basic GPWS uses the aircraft's downward-looking radar altimeter to identify an excessive rate of descent or closure with terrain, and then provides an audible warning in the cockpit. Since 2007, virtually all commercial aircraft have enhanced GPWS, known as terrain awareness and warning system (TAWS), which uses a terrain database to show terrain on the FMS navigation map display, and to give earlier warning of terrain closure

Figure 3.3 shows the scenario in the form of a barrier model. The initiating event is an incorrect trajectory command. A CFIT occurs if all barriers are unsuccessful. The reasons for the barriers being unsuccessful are the causes of the CFIT accident, and identified in the full fault tree report [2] and in EUROCONTROL's IRP [11]. They are modelled in the fault tree described below.

**Figure 3.3 CFIT Barrier Model**

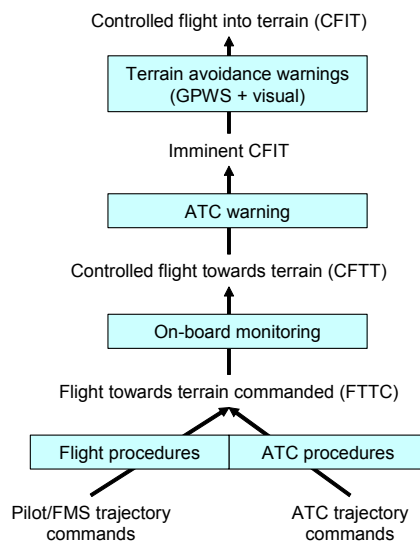
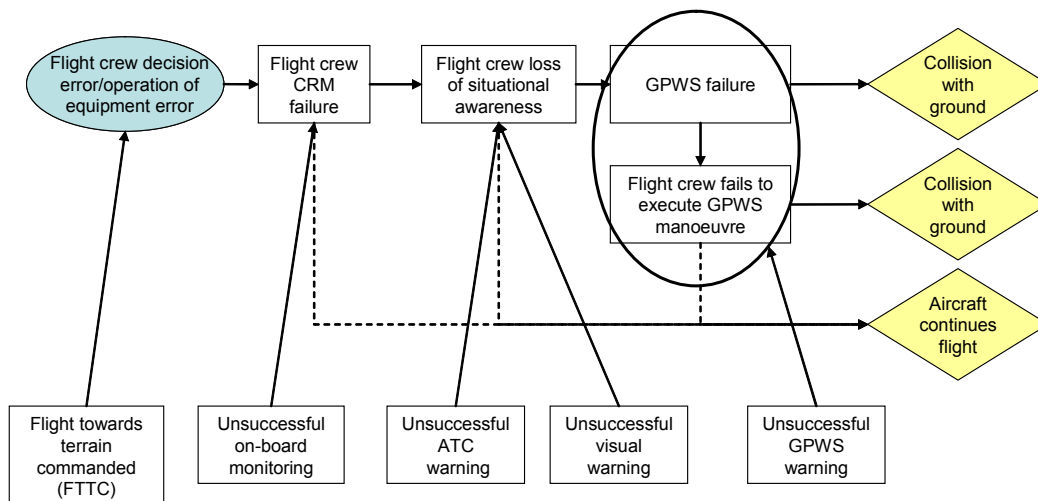


Figure 3.4 shows the mapping between the barrier model and the ESD model. Despite some differences in terminology, the two models are broadly equivalent and numerically identical.

**Figure 3.4 Mapping from Barrier Model to ESD of CFIT**



### 3.5 CFIT Accident Frequency

The frequency of CFIT accidents is based on 152 accidents among Western commercial aircraft world-wide during 1990-2005, as recorded in the ADREP database. The number of flights by such aircraft in this period is estimated as 453 million [2], so the accident frequency is estimated as  $3.4 \times 10^{-7}$  per flight.

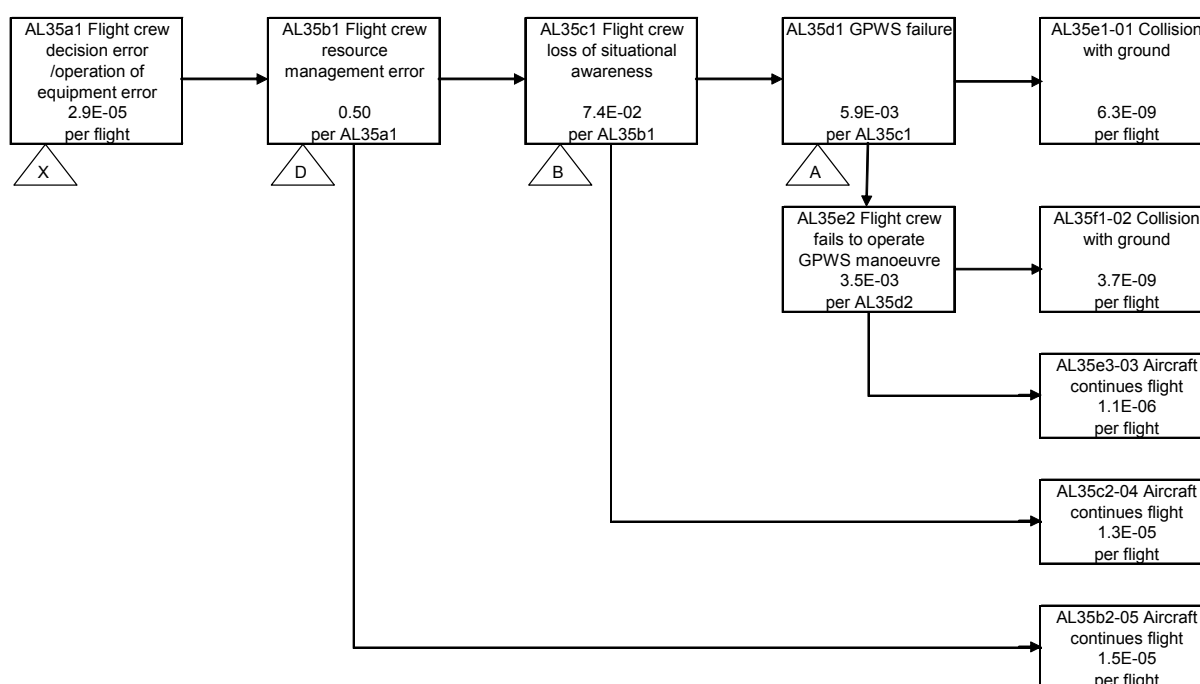
During the data period, there has been a declining trend in the accident frequency. Analysis of possible causes suggests this is mainly due to changes in GPWS type and fitment over this period. Since TAWS is now required for virtually all commercial aircraft, the fault tree model presented below is for a reference case consisting of TAWS-equipped aircraft.

To date, there have not been any CFIT accidents on TAWS-equipped commercial aircraft [15]. Assuming they were 70% of their way to the first accident by the end of 2005, their accident frequency is estimated as  $6.4 \times 10^{-9}$  per flight [2]. Recognising the large uncertainty in this estimate, it is rounded to  $1 \times 10^{-8}$  per flight. This means that the frequency estimate would not increase unless two accidents occurred on TAWS-equipped aircraft.

### 3.6 Quantified ESD

The quantified ESD for CFIT on TAWS-equipped aircraft is shown in Figure 3.5. Combination of the two end events involving collision with the ground (AL35e1-01 and AL35f1-02) gives the above frequency of  $1 \times 10^{-8}$  per flight.

Figure 3.5 ESD for CFIT



The values of the ESD events above are slightly different from the ones used in the fault tree package that was supplied for the CATS model. They differ from the quantified ESD report [1] due to validation (Section 3.11). They are taken from the CFIT report [2], and refer to TAWS equipped aircraft. The values provided for the CATS model include a small proportion (0.5%) of aircraft with no GPWS fitted.

The ESD shows:

- The frequency per flight of the initiating event, which is an incorrect trajectory command for flight towards terrain.
- The probability per demand for each of the pivotal events (i.e. unsuccessful barriers).
- The frequency per flight for each of the end events.

Quantification of the branching probabilities is based on failure experience with and without GPWS, independent estimates of failures of on-board monitoring, ATC warning and visual warning [2]. The initiating event frequency has been deduced from the combination of these parameters, ensuring that the correct CFIT frequency is retained.

### 3.7 Causal Data

In order to construct the fault tree model, the following groups of accidents and incidents have been analysed:

- Fatal CFIT accidents involving large Western commercial jets during 1990-2005. This dataset includes all 37 known accidents of this type, occurring world-wide. This dataset is chosen because it is comprehensively reported and because causal investigations are available for many of the events.
- Controlled flight towards terrain (CFTT) incidents involving commercial aircraft during 2000-2005. This dataset consists of 11 incidents for which comprehensive reports are available in the public domain. The incidents include large Western commercial jets and also some turboprops. This dataset is used to ensure the causal distributions in the model reflect all types of commercial aircraft.
- CFTT incidents recorded in the British Airways BASIS system during 1997-2001. This dataset consists of 37 incidents on large Western commercial jets and some turboprops. This dataset is chosen because it covers incident precursors, which are too minor to be covered in the other datasets, but which are potentially suitable for monitoring in airline operations.

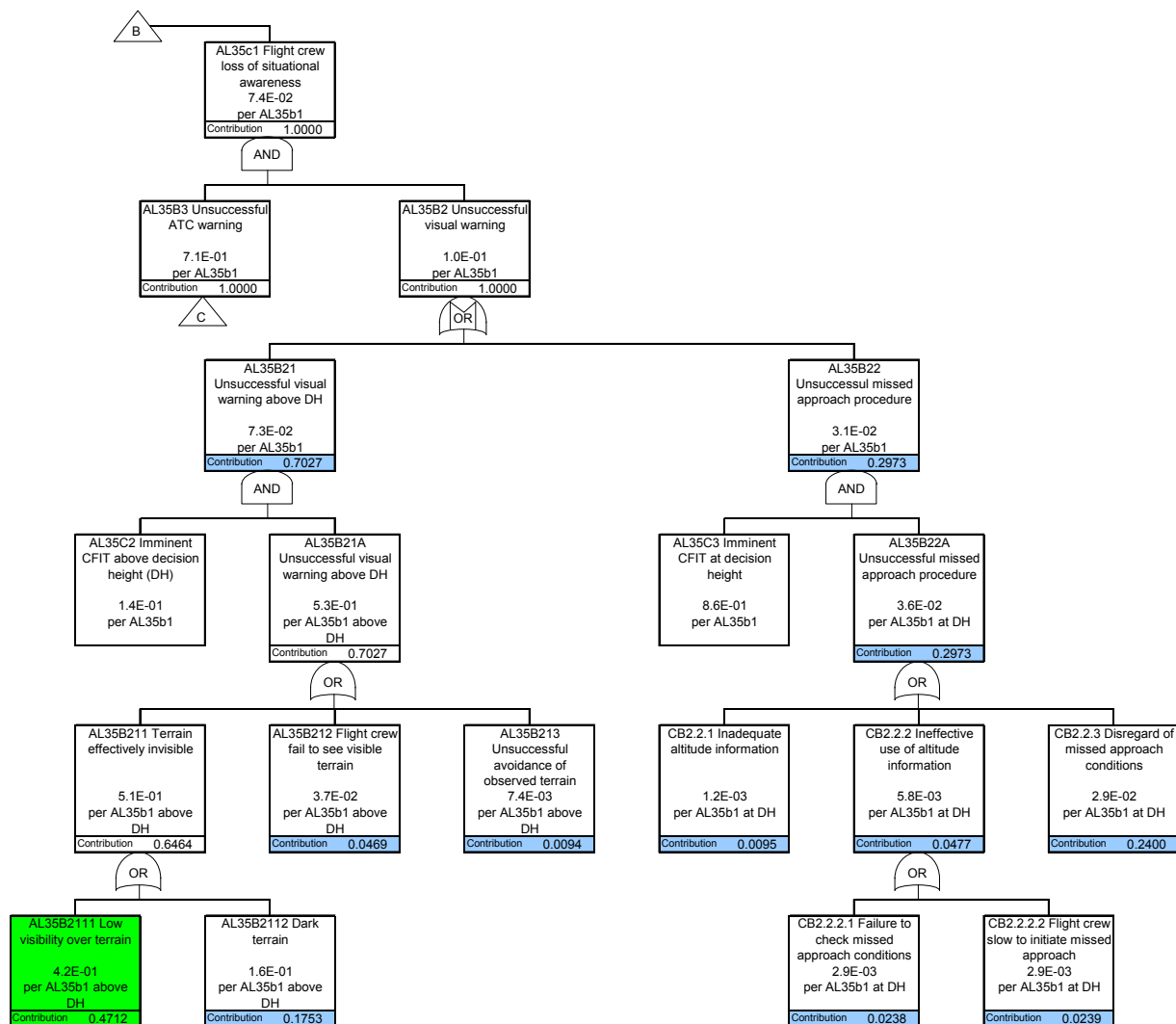
In total 85 accidents and incidents have been analysed in detail, identifying the causes of failure of each barrier. The analysis is documented in the full report [2]. Each fully-investigated CFIT accident gives information on the causes of failure of all 5 barriers. In each incident, at least one barrier was successful, but they each give information on the causes of at least one barrier failure. In future work, it would be desirable to enlarge these datasets by analysing more causal investigations of CFIT accidents and CFTT incidents. It would be desirable to include non-fatal accidents, and events on turboprops, small commercial jets and Eastern-built aircraft, to better represent the whole set of commercial aircraft.

### 3.8 CFIT Fault Tree

Fault trees have been developed by DNV for the initiating event and each of the pivotal events [2]. Figure 3.6 shows an example for the pivotal event "loss of situational awareness". This is considered equivalent to the barriers "ATC warning" and "visual warning".

The values of the fault tree events are the ones used in the fault tree package that was supplied for the CATS model. They are identical to the values in the CFIT report [2], but following validation (Section 3.11) they differ from the quantified ESD report [1].

Figure 3.6 Fault Tree for Visual Warning



For each event, the tree shows:

- The failure probability per demand. In general, the events are conditional on occurrence of events to the left of them in the tree.
- The contribution of the event to the failure of the barrier and hence to CFIT (defined in Section 2.4.4).

The fault tree uses colour coding to indicate the pedigree of the probability and contribution for each event. Four categories are distinguished:

- Probabilities based directly on probability data (the most robust) - green.
- Contributions based on the distribution of causal factors in an accident dataset - blue.
- Probabilities and contributions deduced from other events - white.
- Probabilities based on pure judgements in the absence of any useful data (the least robust) - yellow.

### 3.9 Uncertainties

Uncertainties in all base events have been quantified as explained in the fault tree report [2]. For example, the best-estimate of world average CFIT accident frequency on commercial aircraft during 1990-2005 is  $3.4 \times 10^{-7}$  per flight. Three known sources of uncertainty, expressed as fractions of the best-estimate value (BE), are:

- Data quantity (90% confidence range based on 152 events) - 0.87 to 1.14x BE.
- Data bias due to accident inclusion criteria - 0.95 to 1.31x BE.
- Data choices in estimation of exposure - 0.85 to 1.13x BE.

The overall (epistemic) uncertainty in the average accident frequency is estimated from the widest range among these known sources as 0.85 to 1.31x BE.

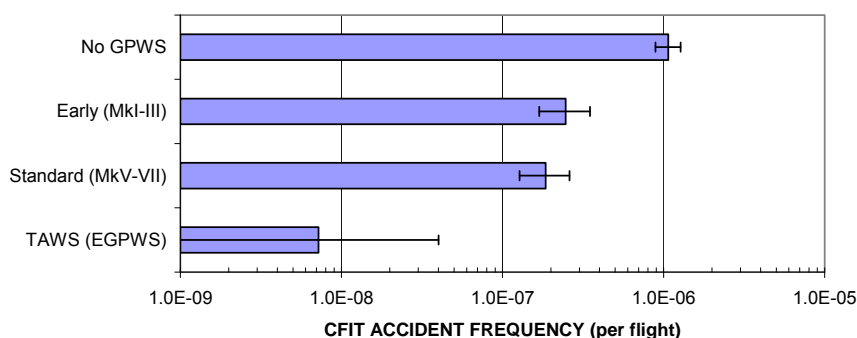
In the case of the causal factors within the fault tree, which are based on splitting the available causal data to the greatest practical extent, the dominant uncertainties usually arise from the small data quantity.

### 3.10 Case-Specific Modifications

The fault tree above represents a generic average set of frequencies and causal breakdowns for commercial aircraft world-wide. Case-specific modifications can be adopted to represent specific cases such as flight phases or aircraft operators through adjustments to the base event probabilities compared to average values. The possible modifications also define the variability in the base event probabilities.

The effects of specific influences on CFIT frequencies have been quantified through a statistical analysis of 152 CFIT accidents obtained from the ADREP database. A total of 17 influencing factors have been identified, for which the accident and flight exposure data can be stratified. Figure 3.7 shows example results for the influence of GPWS type.

**Figure 3.7 Effect of GPWS on CFIT Accident Frequency**



Different influencing factors can be compared in the form of risk ratios, obtained by dividing by the average frequency. Table 3.1 compares and ranks the risk ratios for the 17 different factors. It shows that GPWS type, approach guidance, cloud amount and visibility restrictions are the most important factors when considered individually.

**Table 3.1 Ranking of Factors Influencing CFIT Frequency**

FACTOR	MAXIMUM RISK RATIO	MINIMUM RISK RATIO	VARIABILITY RATIO	RANKING
Aircraft type	2.0	0.6	1.8	15
Aircraft size	1.6	0.5	1.7	16
Aircraft generation	1.8	0.4	2.0	14
GPWS type	3.2	0.02	12.2	1
Geographical region	5.2	0.3*	4.0	5
National income	3.8	0.3	3.4	7
Airport elevation	3.3	0.5	2.5	9
Approach guidance	9.4	0.2	6.2	3
Terminal area radar	3.1	0.8	2.0	13
Light condition	1.7	0.7	1.5	17
Cloud amount	6.9	0.2	6.5	2
Precipitation	10.1	0.7	3.9	6
Visibility restrictions	8.2	0.3	5.3	4
Captain's experience	1.7	0.2	3.1	8
First Officer's experience	1.4	0.3	2.0	12
Difference in crew experience	1.5	0.3	2.4	11
Operation type	3.6	0.6	2.5	10
Overall	10.1	0.02	21.8	

The overall variability in the average accident frequency is estimated from the widest range among these influences as 0.02 to 10.1x BE. This is a range of 500-fold.

In the model, the effects of GPWS type are re-normalised to refer to a basis of TAWS-equipped aircraft, for consistency with the ESD. The effects of approach guidance are also used directly in the model (Appendix I). Because most other influences affect crew errors or aircraft reliability, which are expected to depend on the influence but not on the accident type, they are represented by average effects for all accident types, rather than specific effects for CFIT (see Appendix I).

### 3.11 Validation

Because the ESD for CFIT was quantified in the DNV fault tree development [2] before the NLR quantification [1] became available, this created an opportunity for comparison at the interface. For this ESD, it was possible to compare the CFIT accident frequency and the probabilities of the initiating event and each pivotal event.

The differences were categorised as follows:

- A. Errors, which must be corrected. One such error was identified. The correction results in the present ESD differing from the NLR one [1].
- B. Data that is available to one approach but not the other. One such additional data source was identified. Its adoption resulted in the CFIT frequency chosen above.
- C. Choices in the data analysis, which are different between the two approaches, but where no one approach is obviously preferable. These differences are of particular interest, because they indicate epistemic uncertainties, which are difficult to quantify in any other way. Several such differences have been used to quantify the uncertainties in the base events [2].

## 4. LOSS OF CONTROL IN FLIGHT

### 4.1 Definition and Importance

Loss of control (LOC) is defined as events where the flight crew lose control of the aircraft's trajectory. In some cases, control may be recovered and the flight continued. Where control is not recovered, the result is an uncontrolled collision (i.e. crash) with the ground.

The fault tree modelling divides LOC events into those during take-off, landing and in-flight. Accidents during take-off and landing are considered in Section 5 and 6. The in-flight phase includes the following:

- Climb to cruise (from 1500 ft or first power reduction to cruising level)
- Cruise (from top of climb to top of descent, including changes of cruise level)
- Normal descent (from top of descent to initial approach fix)
- Holding (typically at the initial approach fix)
- Low fly-past
- Emergency descent
- Initial approach (from initial approach fix to intermediate approach fix)
- Intermediate approach (from intermediate approach fix to final approach fix)
- Final approach (from final approach fix to runway threshold)
- Missed approach (from terminating approach to rejoining intermediate/final approach)

Loss of control in flight (LOCF) accounted for 19% of fatal accidents and 26% of fatalities among world-wide operations of Western commercial aircraft during 1990-2006.

### 4.2 LOCF Scenarios

The causes of loss of control are characterised by great diversity. They include environmental conditions (e.g. icing, wind-shear, turbulence), technical failures (e.g. engine failure, control system failure), human-technical interaction on-board (e.g. low air speed, fuel exhaustion, flap configuration) and flight handling (e.g. stall practice).

LOC in flight covers 6 of the ESDs, which are:

- ESD12 - flight crew spatial disorientation
- ESD13 - flight control system failure
- ESD14 - flight crew incapacitation
- ESD15 - anti-ice system failure
- ESD16 - flight instrument failure
- ESD37 - wake vortex encounter

The DNV report [3] addresses all of these. As an example, the present report covers only ESD12 (spatial disorientation).

Another cause of loss of control in flight (ESD18 - engine failure ) is addressed separately in Section 7.

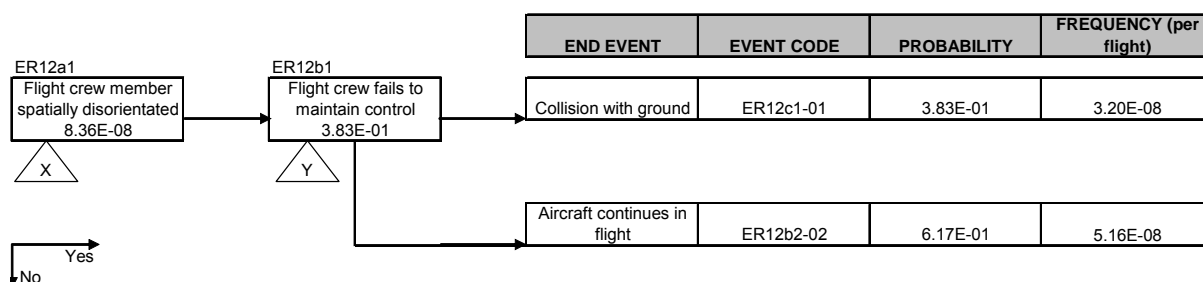
### 4.3 Event Sequence Diagram

Spatial disorientation refers to a scenario where the flight crew develop a mistaken perception of their position and motion. This may induce flight commands that place the aircraft in an extreme attitude, outside the normal flight envelope, i.e. unusual bank or pitch angles. Unless this attitude is corrected, it is virtually impossible for the flight crew to control

the aircraft's trajectory, and so in effect control is lost at this point. Controlled flight into terrain (CFIT) is treated separately in ESD35.

The ESD for spatial disorientation has been quantified by NLR [1]. This is shown in Figure 4.1. The fault tree is required to give the causal breakdown for the initiating and pivotal events, highlighted by the labels X and Y.

**Figure 4.1 Event Sequence Diagram for Spatial Disorientation**



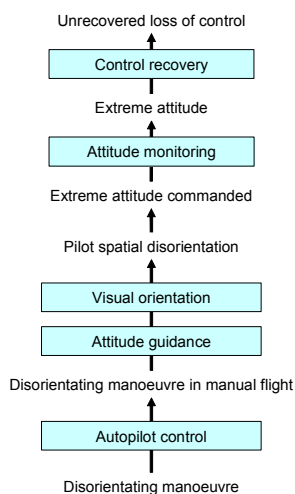
#### 4.4 Barrier Model

The following are the major barriers against LOC due to spatial disorientation, all of which must be unsuccessful if the accident is to occur:

- Autopilot control. Spatial disorientation occurs when the flight crew have manual control of the aircraft trajectory. Modern commercial aircraft have autopilots that can control the trajectory for almost the entire flight except take-off and touch-down. However, to maintain handling practice, pilots often retain manual control in climb to about 10,000ft, and in descent from about 3000ft or on making visual contact with the runway.
- Attitude guidance. In instrument flight rules (IFR), the flight instruments are the primary mechanism for maintaining spatial orientation. The key instrument is the attitude director indicator (ADI). Commercial aircraft are fitted with 3 ADIs, one each for PF and PNF, and a spare that can be selected by either pilot.
- Visual orientation. In visual meteorological conditions (VMC), the pilot's ability to see the horizon assists in maintaining spatial orientation.
- Attitude monitoring. The pilot not flying (PNF) should monitor the actions of the pilot flying (PF) and challenge any incorrect attitude commands before the aircraft reaches an extreme attitude.
- Control recovery. If the aircraft reaches an extreme attitude, it remains possible for pilots to correct it, but this requires actions for which only military or aerobatic pilots are trained, as there is a danger of inducing structural failure through incorrect commands.

Figure 4.2 shows the barrier model for spatial disorientation. It shows a sequence of accident precursors, which the different barriers attempt to prevent developing into the accident.

**Figure 4.2 Barrier Model of Spatial Disorientation**



#### 4.5 Causes of Barrier Failure

Each of the 5 barriers may fail (i.e. be unsuccessful in preventing the scenario developing to the next precursor) for different reasons. The reasons for barrier failure are represented in the fault tree as the causes of the accident. Thus the model represents at least 5 causes of any accident due to spatial disorientation.

The causes of barrier failure are identified in full in the DNV report [3]. As an example, considering only the first barrier, the identified causes of lack of autopilot control are:

- Autopilot not capable of controlling the aircraft in the required manoeuvre. This typically occurs on older or smaller aircraft where the autopilot is only suitable for steady flight conditions.
- Autopilot not used by the flight crew. This may be due to:
  - Training (or maintaining familiarity) of the flight crew in manual flight.
  - Crew preference for manual flight.
  - Crew lack of knowledge of how to use the autopilot to control the aircraft in the required manoeuvre.
- Autopilot incorrectly used by the flight crew. This is where the flight crew attempt to use the autopilot but fail to achieve control over the aircraft trajectory with it.

The model represents these as alternative causes of failure of the first barrier. The underlying human and organisational reasons for these events are not suitable for modelling in the fault trees. The development of causes in the fault tree therefore stops at the point where reasonably distinct independent events can be identified that are either necessary or sufficient to cause failure of a barrier.

#### 4.6 LOCF Data

Spatial disorientation events are difficult to identify from available databases such as ADREP. Therefore, events have been accumulated through a slow process of categorising

loss of control events into the different ESDs. Ten spatial disorientation accidents were obtained for preliminary quantification. More recently, further events have been identified and could be used in future work. Significant uncertainty results from the use of such a small dataset, as considered further below.

Each event has been analysed to determine the cause of failure of each barrier. Table 4.1 shows this analysis for an example spatial disorientation accident. Each cause is assigned to the events identified for the fault tree. Analysis of sufficient events creates the required causal distributions. The analysis of all accidents is documented in full in the DNV report [3].

**Table 4.1 Example Spatial Disorientation Accident**

<b>Date</b>	23 Aug 00	
<b>Type</b>	A320	
<b>Operator</b>	Gulf Air	
<b>Location</b>	Bahrain	
<b>Flight phase</b>	Missed approach	
	<b>Description of failure</b>	<b>Fault tree event</b>
<b>Visual orientation</b>	Conditions were darkness with no moon but good visibility.	Darkness
<b>Autoflight system</b>	The aircraft was making a VOR/DME approach. At 1700ft the autopilot was disconnected when visual with the airfield.	Autopilot not capable.
<b>Attitude guidance</b>	The aircraft was fast on approach, and while at 600ft used a non-standard 360° turn to reduce speed, but then made a missed approach. During this, the captain became spatially disorientated, falsely perceiving the aircraft was pitching up. He commanded the aircraft into 15° nose-down pitch, while at only 1000ft altitude.	ADI not used.
<b>Attitude monitoring</b>	The first officer (PNF) had not alerted the captain to the non-standard elements of the approach, in contravention of operating procedures. When the nose-down pitch was commanded, the speed increased and the Master Warning indicated flap speed exceeded, which the first officer called out, but the captain did not respond to this.	Lack of monitoring.
<b>Control recovery</b>	GPWS pull-up warnings were received. The captain then responded only by raising the flaps.	Incorrect recovery action.
<b>Consequences</b>	The aircraft struck the sea at 280 knots.	

**4.7 LOCF Fault Tree**

The fault tree for spatial disorientation is given in full in Figures 4.3 and 4.4. For each event, the tree shows the failure probability per demand. In general, the events are conditional on occurrence of events to the left of them in the tree. For the events on the extreme left side, the relevant demand is a flight.

**Figure 4.3 Top Events of Fault Tree for Spatial Disorientation**

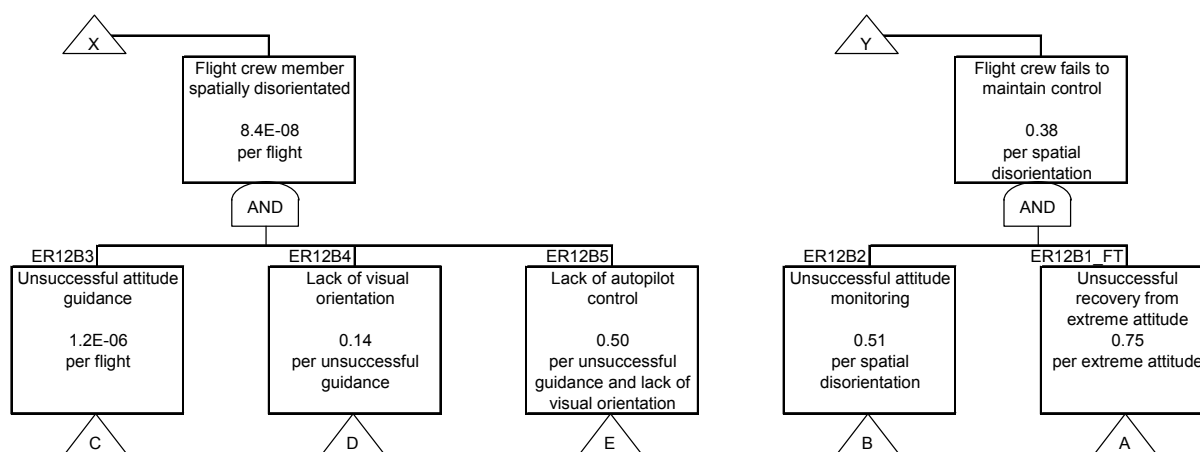


Figure 4.4 Base Events of Fault Tree for Spatial Disorientation

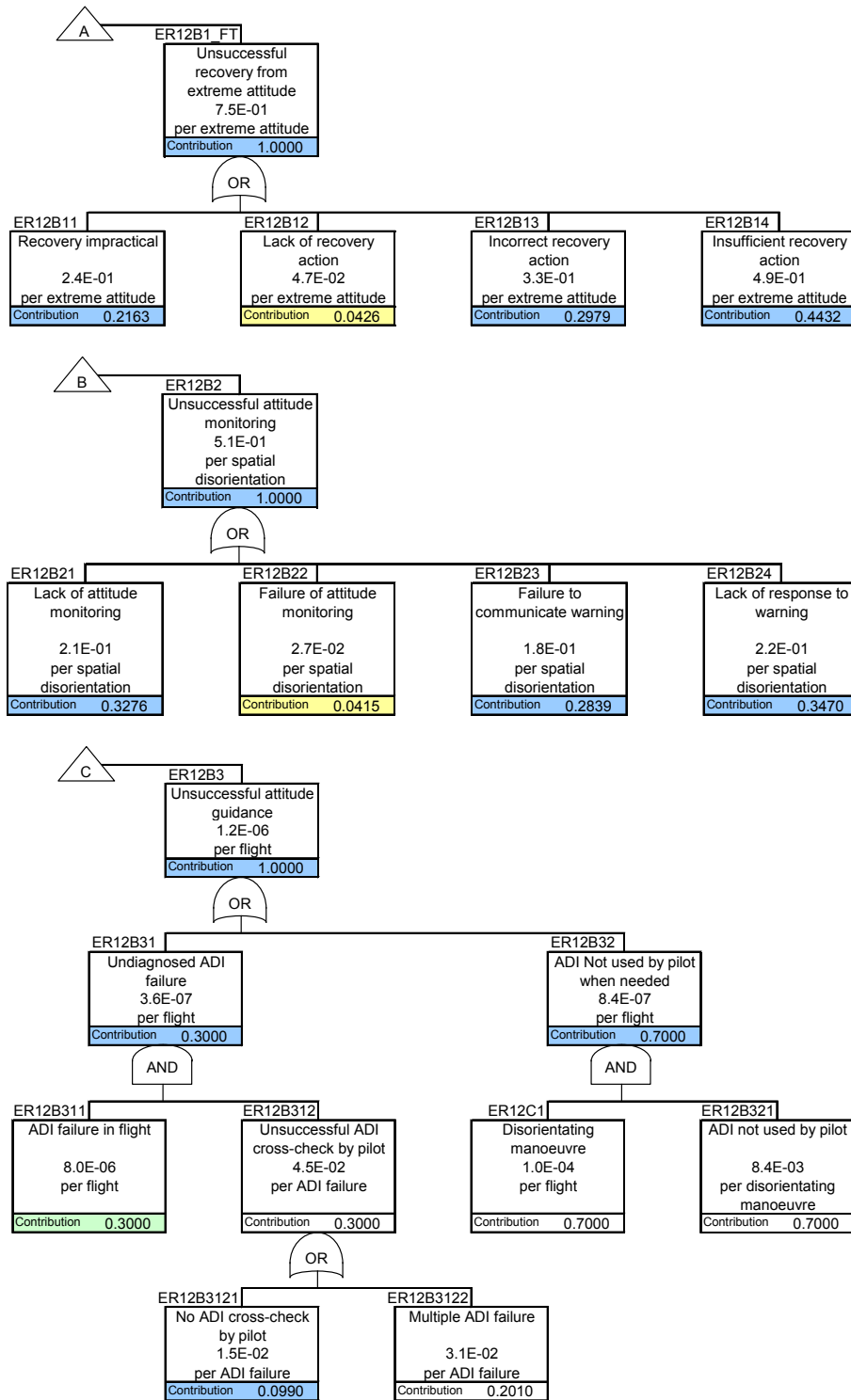
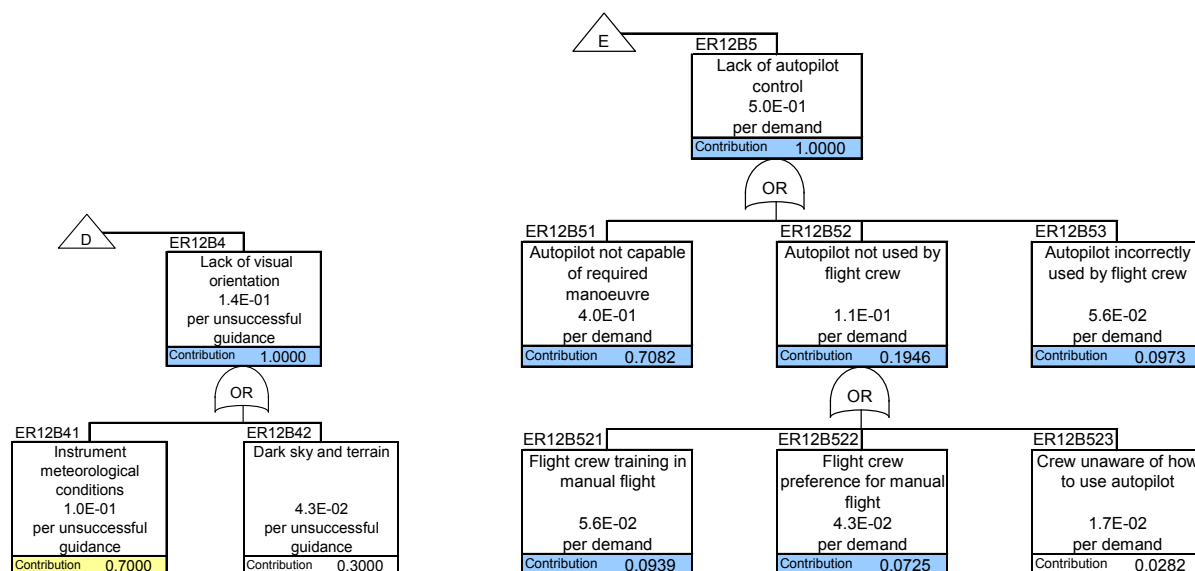


Figure 4.4 Base Events of Fault Tree for Spatial Disorientation (cont'd)



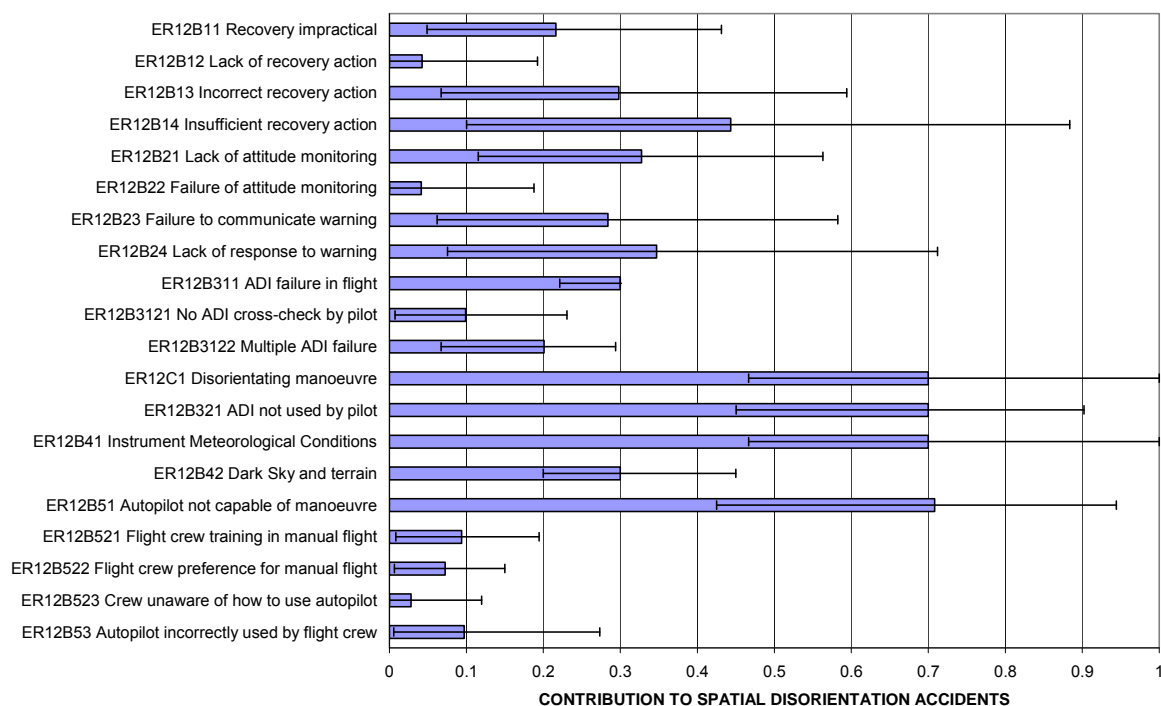
The values of the fault tree events above are the ones used in the fault tree package that was supplied for the CATS model. They differ from the values in the LOCF report [3] because they have been adjusted to match the quantified ESD report [1]. The differences are discussed in the validation exercise in Section 4.11. For simplicity, the fault tree reports [3-9] have not been updated, because the methodology remains the same. The parameters that were adjusted in this way are recorded in the documentation in the fault tree package, which is copied into the CATSPAWS parameter database.

#### 4.8 Contributions

Figure 4.5 shows the contributions from the base events of the spatial disorientation fault tree. They are expressed as contributions to the spatial disorientation accident frequency, as shown in the fault tree. The 90% confidence ranges shown on these results are based on epistemic uncertainties.

Such results provide potentially useful information about the relative importance of different causal factors. For example, the results above suggest that pilot failure to use the ADI is a more common cause of spatial disorientation than failure of the ADI. It also shows that most spatial disorientation accidents involve disorientating manoeuvres (e.g. turns during missed approach) in IMC under manual flight control. This shows areas in which safety improvements could be concentrated. These are also areas in which the model could be made more detailed in future work.

**Figure 4.5 Contributions from Base Events of Fault Tree for Spatial Disorientation**



**Table 4.1 Base Event Influences for Spatial Disorientation**

CODE	EVENT NAME	FLIGHT CREW PERFORMANCE	ATCO PERFORMANCE	MAINTENANCE PERFORMANCE	OTHER INFLUENCES
ER12B11	Recovery impractical				
ER12B12	Lack of recovery action	x			
ER12B13	Incorrect recovery action	x			
ER12B14	Insufficient recovery action	x			
ER12B21	Lack of attitude monitoring	x			
ER12B22	Failure of attitude monitoring	x			
ER12B23	Failure to communicate warning	x			
ER12B24	Lack of response to warning	x			
ER12B311	ADI failure in flight			x	
ER12B3121	No ADI cross-check by pilot	x			
ER12B3122	Multiple ADI failure			x	
ER12C1	Disorientating manoeuvre				Airport quality
ER12B321	ADI not used by pilot	x			
ER12B41	Instrument Meteorological Conditions				Visibility in flight
ER12B42	Dark Sky and terrain				Light condition
ER12B51	Autopilot not capable of manoeuvre			x	Autoflight use
ER12B521	Flight crew training in manual flight				
ER12B522	Flight crew preference for manual flight				
ER12B523	Crew unaware of how to use autopilot	x			
ER12B53	Autopilot incorrectly used by flight crew	x			

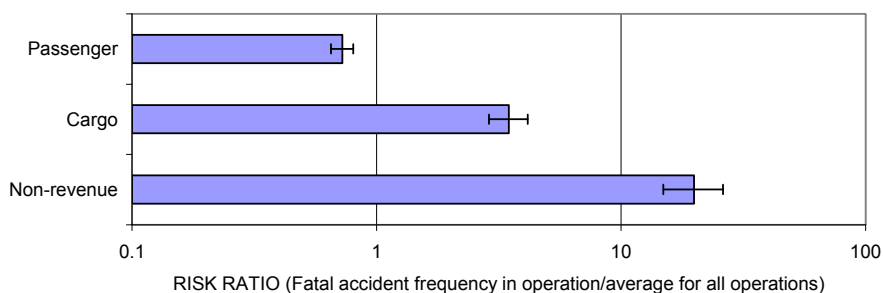
#### 4.9 Case-Specific Modifications

The fault tree above represents a generic average set of frequencies and causal breakdowns for commercial aircraft world-wide. Case-specific modifications can be adopted to represent specific cases such as flight phases or aircraft operators through adjustments to the base event probabilities compared to average values. Some key influences (notably the

standard of performance of flight crew, ATC and maintenance personnel) are quantified by human performance BBNs elsewhere in the CATS model. The influences of these parameters are represented by conditioning the BBN to particular values within the distributions. Their effect on the fault tree is assumed to be the same for each base event that has a logical connection to the human performance. Example connections for base events from part of the spatial disorientation fault tree are shown in Table 4.1

Other influences are identified in Table 2.2, and quantified in Appendix I. Figure 4.6 illustrates these using operation type as an example influence. The number of fatal accidents in each operation has been obtained from the ADREP database for Western commercial aircraft during 1990-2006. After dividing by the estimated number of flights in each operation, the results are expressed as a risk ratio relative to average. Fatal accidents have been selected to avoid bias due to uneven reporting of non-fatal accidents. The example shows that risks on passenger operations are significantly lower than average, while in cargo and non-revenue operations they are significantly higher than average. Modification factors for specific cases are based on the necessary adjustments of the base events in the model to produce the risk ratios that are shown in the data. It is further assumed that operation type affects all base events influenced by flight crew and maintenance performance (as shown in Table 4.1).

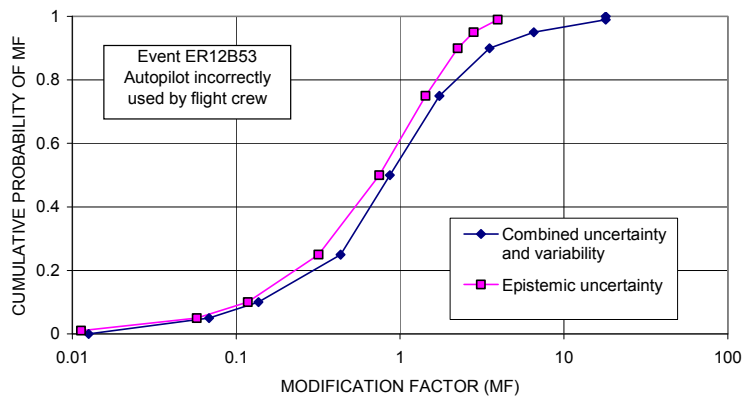
**Figure 4.6 Example Risk Ratios from Accident Data**



#### 4.10 Uncertainties

Figure 4.7 shows the uncertainty distributions for an example base event in the spatial disorientation model. This event probability is based on only one accident, and so the epistemic uncertainty is large, with a 90% range covering nearly two orders of magnitude. The variability between flights is also large, and highly skewed (it appears symmetrical in the plot, but only because this uses a log scale), although the distribution is truncated at a value of 18, when the event probability reaches its maximum of 1. The variability dominates the combined distribution for large MFs.

**Figure 4.7 Uncertainty Distributions for Example Event**



#### 4.11 Validation

Because the ESD was quantified in the DNV fault tree development [3] before the NLR quantification [1] became available, this creates an opportunity for comparison at the interface. For this ESD, it is possible to compare the spatial disorientation accident and incident frequencies as follows:

- The NLR accident frequency is 1.7x higher than the DNV value.
- The NLR incident frequency is 1.5x lower than the DNV value.

Both sets of differences are considered to be mainly Type C (using the classification from Section 3.9), reflecting the overall uncertainty in the result. These are within the uncertainties estimated from the data quantity.

## 5. LOSS OF CONTROL IN TAKE-OFF

### 5.1 Definition and Importance

Loss of control in take-off (LOCT) covers the following flight phases:

- Take-off run (from application of take-off power to 50 ft above runway)
- Aborted take-off (take-off terminated between application of take-off power and 50 ft above runway)
- Initial climb (from 50 ft above runway to 1500 ft or first power reduction)

Loss of control in take-off (LOCT) accounted for 8% of fatal accidents and 9% of fatalities among world-wide operations of Western commercial aircraft during 1990-2006.

### 5.2 LOCT Scenarios

In order to quantify the risks, LOC accidents are categorised into characteristic scenarios, represented by ESDs [1]. LOC in take-off covers 10 of the ESDs, which are:

- ESD1 - aircraft system failure
- ESD2 - ATC event
- ESD3 - flight crew handling
- ESD4 - directional control system failure
- ESD5 - flight crew system operation
- ESD6 - contaminated wing
- ESD7 - aircraft outside weight and balance limits
- ESD8 - windshear
- ESD9 - engine failure
- ESD10 - pitch control problem

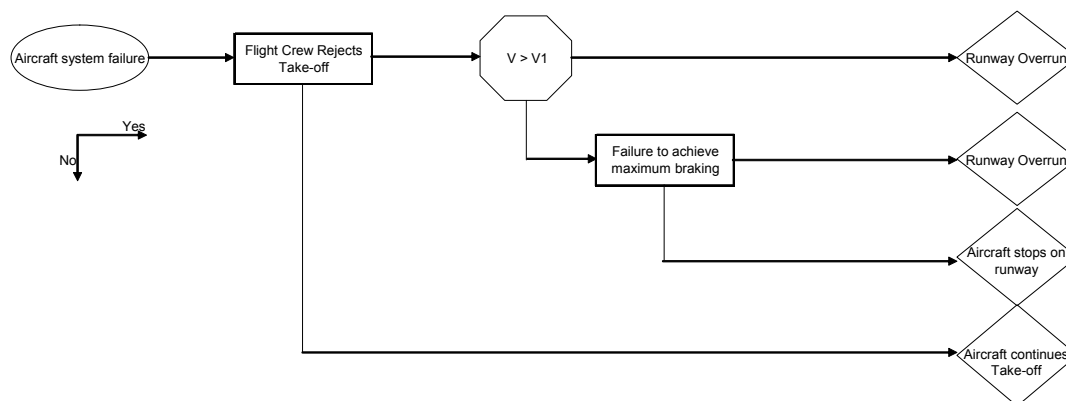
The DNV report [5] addresses all of these. As an example, the present report covers only ESD 1 (aircraft system failure).

### 5.3 Event Sequence Diagram

Figure 5.1 shows the scenario as represented in the NLR ESD [1]. The possible end events of the ESD are:

- Runway overrun after the flight crew incorrectly rejects take-off above  $V_1$ .
- Runway overrun after the flight crew correctly rejects take-off below  $V_1$  but fails to achieve maximum braking.
- Aircraft stops safely on the runway.
- Aircraft continues take-off and begins flight with system failure. This may become an initiating event for a forced landing scenario.

**Figure 5.1 Event Sequence Diagram for Aircraft System Failure**



#### 5.4 Barrier Model

The following are the major barriers against LOCT due to aircraft system failure:

- Aircraft system integrity. The systems critical for a safe take-off are designed, manufactured and maintained to ensure that they are operating correctly when required at take-off. The flight crew must operate them correctly and check that they are functioning prior to take-off.
- Take-off rejection. If the aircraft is below  $V_1$  when the aircraft system failure occurs then the take-off must be aborted and the aircraft should be brought to a halt on the runway. If the aircraft is above  $V_1$  when the aircraft system failure occurs then the take-off must be continued.
- Braking. Following take-off rejection at  $V_1$  the braking systems must be operating correctly and correctly applied in order to stop the aircraft within the available runway length and prevent an overrun.

The reasons for the barriers being unsuccessful are the causes of the LOC accident, and identified in full in the DNV report [5]. They are modelled in the fault tree.

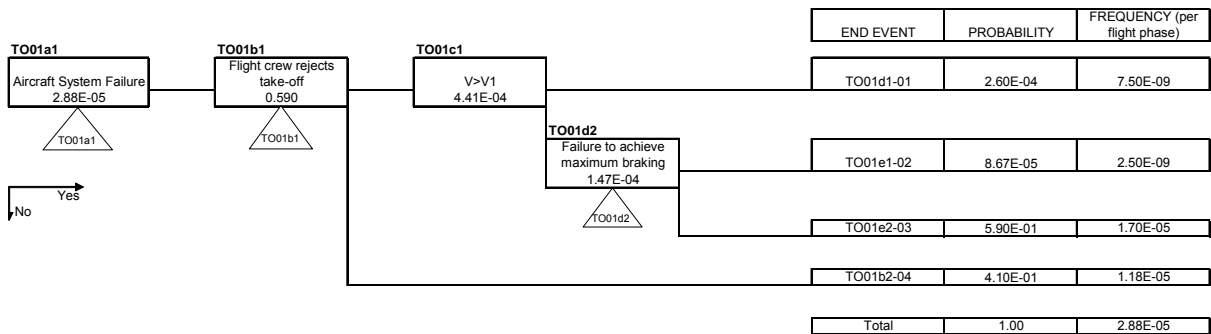
#### 5.5 LOCT Data

The LOCT fault trees are based on an analysis 73 accidents during take-off on large Western commercial jets during 1990-2004. The accidents have been analysed in detail, identifying the causes of failure of each barrier, as documented in the report [5]. Only 3 of these were due to aircraft system failure. These are therefore supplemented by analysis of the full dataset where appropriate, and by Service Difficulty Report (SDR) data on system failures. In future work, it would be desirable to analyse accidents on other commercial aircraft and near miss incidents involving aircraft system failures.

#### 5.6 LOCT Fault Tree

Figure 5.2 shows the quantified version of the ESD for aircraft system failure, taken from the NLR report [1]. This is the starting point for the fault tree development.

Figure 5.2 Event Tree for ESD 1 – Aircraft System Failure



Fault trees have been developed by DNV for each of the barriers [5], as shown in Figures 5.3 - 5.4. These use the same colour coding of pedigree as above. The fault tree for the initiating event is not shown, as it simply combines 14 different SDR event frequencies. There is no fault tree for the  $V > V_1$  event as it is a physical condition and is just a probability with no underlying causes. It should be noted that at the present there is scant data or information to support many parts of the quantification. It would be desirable to obtain further information to update them.

Figure 5.3 Fault Tree – Take-off Rejection

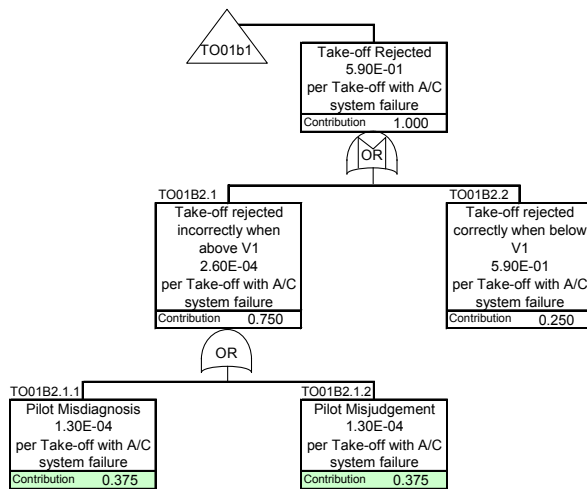
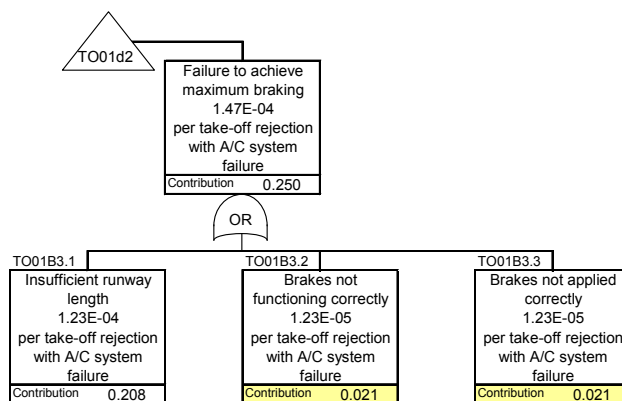


Figure 5.4 Fault Tree – Failure to Achieve Maximum Braking



The values of the fault tree events above are the ones used in the fault tree package that was supplied for the CATS model. They differ from the values in the LOCT report [5] because they have been adjusted to match the quantified ESD report [1].

### **5.7 Case-Specific Modifications**

Analysis of ADREP data for take-off accidents showed influence effects that were similar to other accident types. Therefore, modification factors are based on data for all accident types considered together, as in Appendix I.

## 6. LOSS OF CONTROL IN LANDING

### 6.1 Definition and Importance

Loss of control in landing (LOCL) covers the following flight phases:

- Landing flare (from runway threshold to touchdown)
- Landing roll (from touchdown to standstill)

LOCL includes accidents where the damage occurs during landing as the result of causes that occur during the approach phase. Accidents during approach where control is lost and the aircraft impacts terrain prior to the runway threshold are covered under LOCF (Section 4). Accidents during approach where the aircraft remains under control until impacting terrain are included under LOCL, or under CFIT (Section 3) if the point of impact is more than 500m before the threshold.

LOCL accounted for 16% of fatal accidents and 9% of fatalities among world-wide operations of Western commercial aircraft during 1990-2006.

### 6.2 LOCL Scenarios

In order to quantify the risks, LOC accidents are categorised into characteristic scenarios, represented by ESDs [1]. LOC in landing covers 9 of the ESDs, which are:

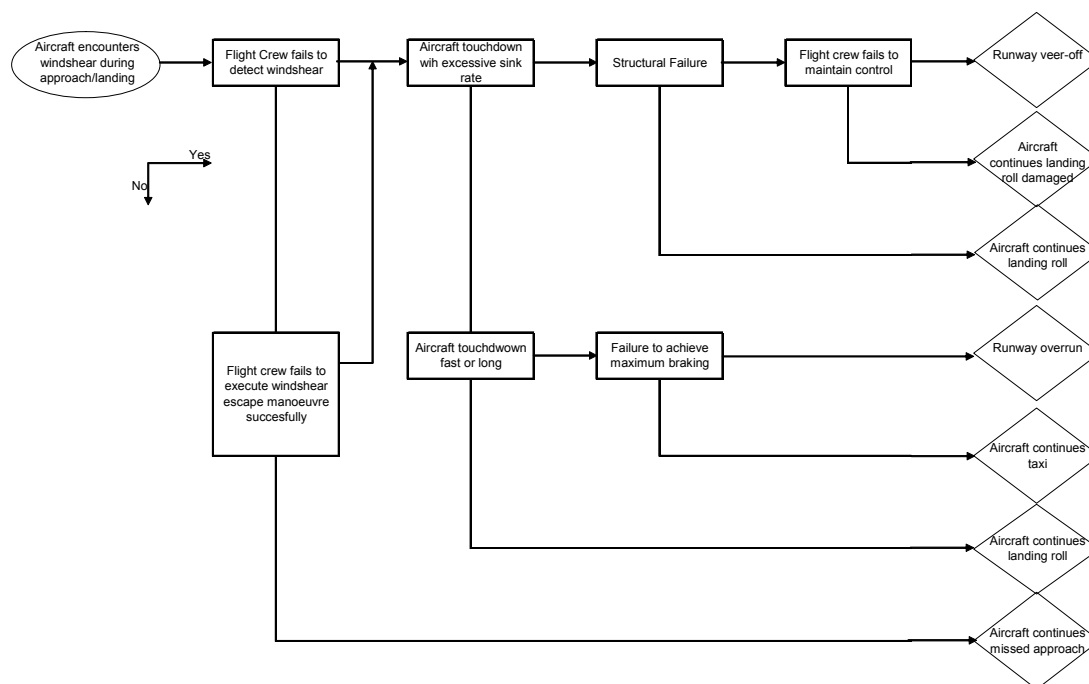
- ESD 19 – unstable approach
- ESD 21 – aircraft weight and balance outside limits
- ESD 23 – windshear
- ESD 25 – incorrect handling during landing flare
- ESD 26 – incorrect handling during landing roll
- ESD 27 – direction control systems failure
- ESD 28 – single engine failure
- ESD 29 – asymmetric thrust reverser failure
- ESD 30 – unexpected wind

The DNV report [4] addresses these. As an example, the present report covers only ESD23 (windshear).

### 6.3 Event Sequence Diagram

Figure 6.1 shows the scenario as represented in the NLR ESD [1]. The fault tree is required to give the causal breakdown for each initiating and pivotal event. Dependencies between the events will be represented by the BBN model.

**Figure 6.1 Event Sequence Diagram for Windshear**



#### 6.4 Barrier Model

The following are the major barriers against LOCL due to windshear:

- Windshear detection and avoidance. Airports vulnerable to windshear may be fitted with a low level windshear alert system (LLWAS). Some aircraft are fitted with airborne predictive windshear systems (PWS). Older aircraft can make use of their weather radar, but these are not specifically designed to give windshear alerts.
- Windshear management. If windshear is encountered during approach the pilot should manage the aircraft to overcome its effects on the aircraft and stabilise the approach. This might include executing a windshear escape manoeuvre.
- Structural strength. The landing gear and surrounding structure are designed to have sufficient strength to prevent damage during moderately hard landing.
- Braking. Aircraft are provided with wheel brakes, spoilers and thrust reversers. The spoilers are required for the wheel brakes to work effectively. In limiting runway conditions, the thrust reversers are also required.
- Control in damaged condition. Even if structural failure occurs, the pilot can still maintain control to keep the aircraft on the runway by applying inputs to the rudder or, in the case of a main gear failure, by attempting to keep the wing up.

The reasons for the barriers being unsuccessful are the causes of the LOC accident, and identified in full in the DNV report [4]. They are modelled in the fault tree.

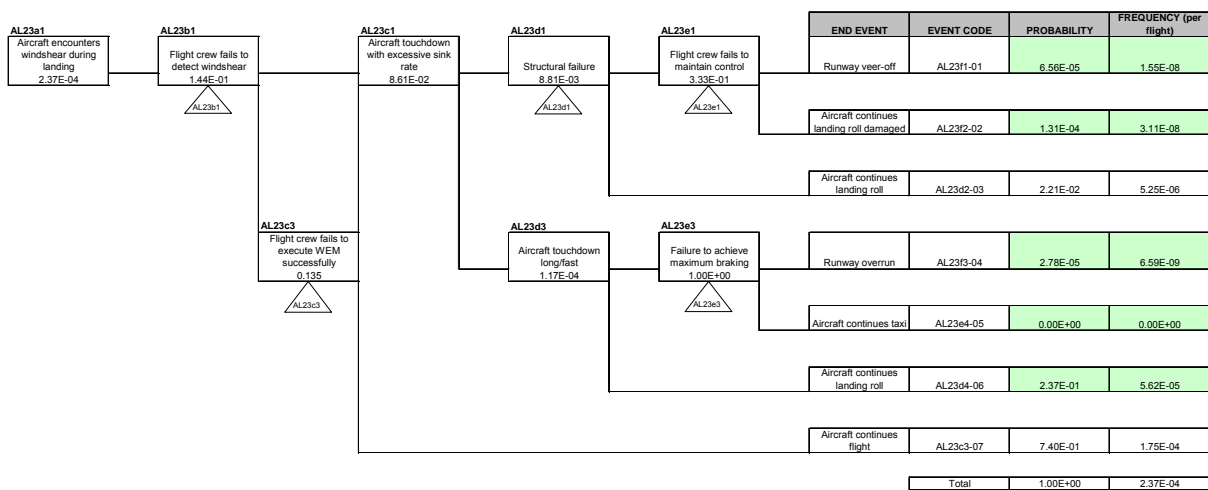
### 6.5 LOCL Data

The windshear fault tree is based on an analysis of just 5 cases of windshear accidents on large Western commercial jets during 1990-2004. Two further windshear accidents in 2005 are not yet reported in sufficient detail to include in the analysis. The 5 selected cases have been analysed in detail, identifying the causes of failure of each barrier, and documented in the report [4]. In future work, it would be desirable to analyse accidents on other commercial aircraft and near miss incidents involving windshear encounters.

### 6.6 LOCL Fault Tree

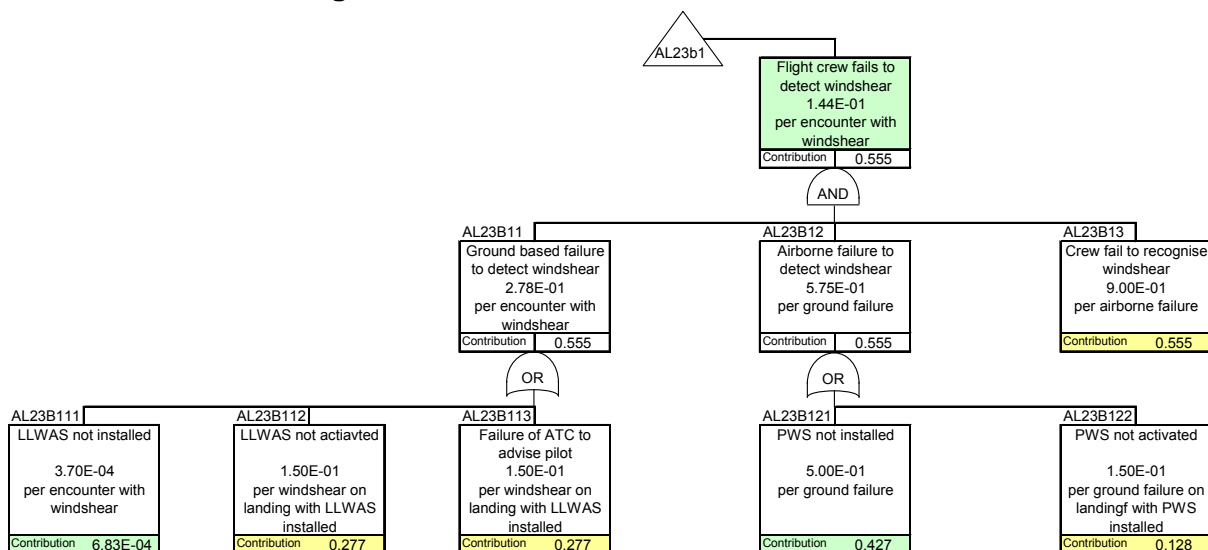
Figure 6.2 shows the quantified version of the ESD for windshear, taken from the NLR report [1]. This is the starting point for the fault tree development.

Figure 6.2 Event Tree for ESD 23 – Windshear

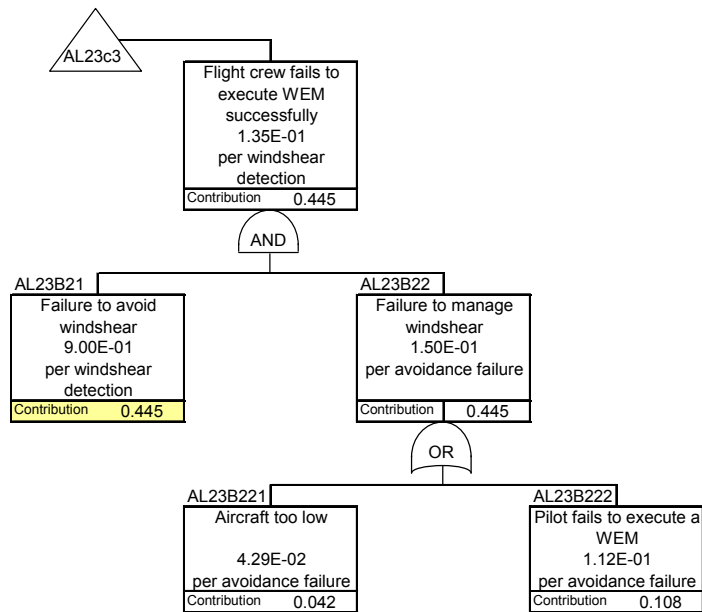


Fault trees have been developed by DNV for each of the barriers as shown in Figures 6.3-6.7. These are based on the original quantification [4], but adjusted to match the pivotal event probabilities from Figure 6.2.

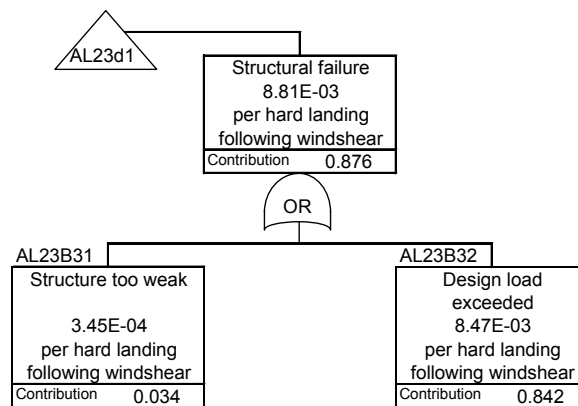
Figure 6.3 Fault Tree – Windshear Detection



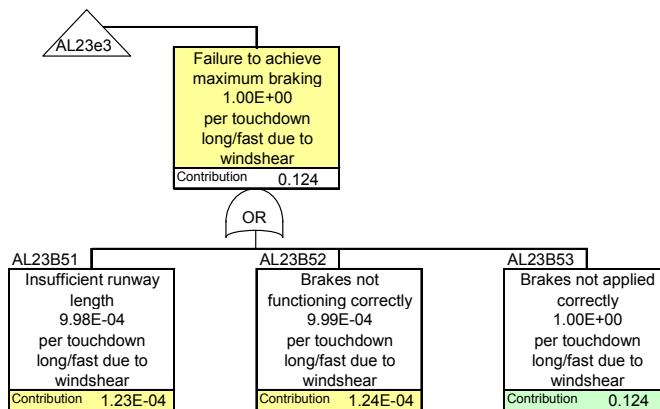
**Figure 6.4 Fault Tree – Windshear Management**



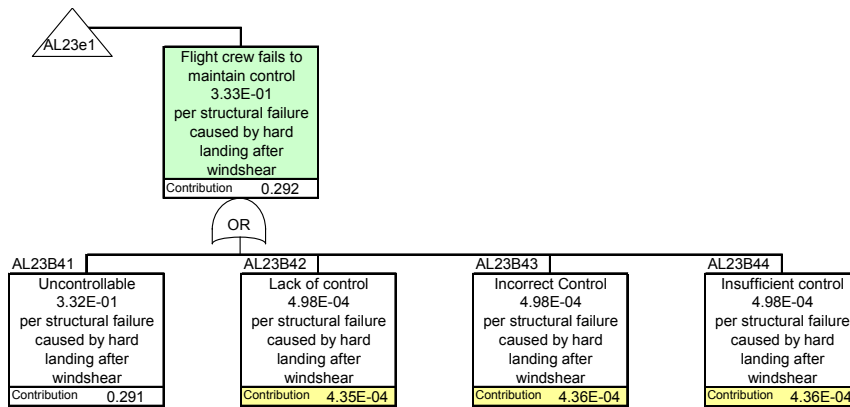
**Figure 6.5 Fault Tree – Structural Strength**



**Figure 6.6 Fault Tree – Braking**



**Figure 6.7 Fault Tree – Control in Damaged Condition**



The values of the fault tree events above are the ones used in the fault tree package that was supplied for the CATS model. They differ from the values in the LOCL report [4] because they have been adjusted to match the quantified ESD report [1].

### 6.7 Case-Specific Modifications

Analysis of ADREP data for landing accidents showed influence effects that were similar to other accident types. Therefore, modification factors are based on data for all accident types considered together, as in Appendix I.

## 7. ENGINE FAILURE IN FLIGHT

### 7.1 Definition and Importance

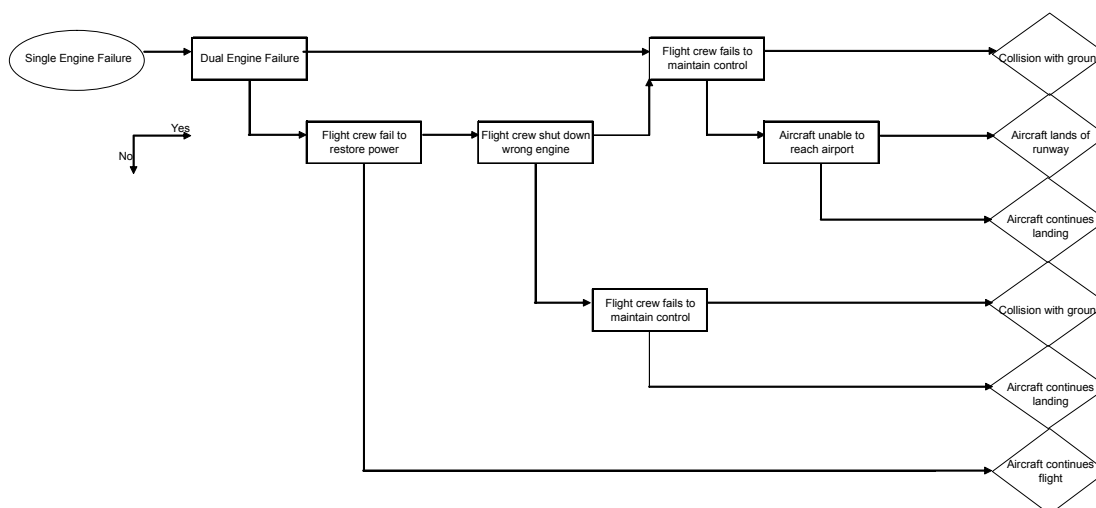
Engine failure in flight (ESD18) is one of the causes of loss of control (LOC) in flight. It is treated separately because many engine failures result in LOC during forced landing. Flight phases are the same as in Section 4.1. Engine failures in take-off are covered under take-off accidents in Section 5.

Loss of control due to engine failure in flight accounted for 16% of fatal accidents and 9% of fatalities among world-wide operations of Western commercial aircraft during 1990-2006.

### 7.2 Event Sequence Diagram

The ESD for engine failure in flight has been specified by NLR [1], as shown in Figure 7.1. The fault tree is required to give the causal breakdown for each initiating and pivotal event. Dependencies between the events will be represented by the BBN model.

**Figure 7.1 Event Sequence Diagram for Engine Failure in Flight**



For simplicity in the ESD, dual engine failure is taken to be total power loss even on aircraft with more than 2 engines.

### 7.3 Barrier Model

The following are the major barriers against LOC due to engine failure in flight:

- Single engine integrity. The integrity of any engine depends on its design, manufacturing and maintenance, and on its operation by the flight crew.
- Multiple engine integrity. Maintaining power following a single engine failure depends on the management of the other engine(s), which will experience increased workload. In some cases the other engine(s) may fail simultaneously with the first, e.g. due to water ingestion.
- Single engine restart. Following the failure of a single engine, provided it is still attached and serviceable, the flight crew should attempt to restart it using the normal

engine start function. If this is unsuccessful, the APU (Auxiliary Power Unit) can be used. When attempting to restart a failed engine, the flight crew should use aircraft warning systems to verify which of the engines has failed, in order to avoid incorrect shutdown of an operable engine.

- Multiple engine restart. Following the loss of power on all engines, the flight crew should attempt to restart them. This may use the normal engine start function, the APU, or as a last resort a windmill restart. This involves placing the aircraft in a rapid descent to force air through the engines in order to increase the revolutionary rate before attempting a restart.
- Control response to partial power loss. Following the failure of a single engine, the aircraft will lose speed and tend to yaw to one side. The flight crew or flight management system must compensate by increasing the thrust on the remaining engine(s) and adjusting the flight control surfaces. If restart fails, the aircraft must then make an emergency landing at a nearby airport.
- Control response to total power loss. Following complete power loss, the flight crew will be only be able to control the aircraft using the flight control surfaces. The loss of power will lead to a reduction in the speed of the aircraft and the flight crew must lose height to prevent the aircraft stalling.
- Forced landing. If control is maintained following the complete power loss, the flight crew may attempt to glide to the nearest airport or, if this is impractical, to an appropriately flat area.

The reasons for the barriers being unsuccessful are the causes of the LOC due to engine failure in flight, and are modelled in the fault tree.

#### **7.4 Engine Failure Data**

The causal breakdown is based on 29 accidents on large Western commercial jets during 1990-2005 involving engine failure in flight. The accidents have been analysed in detail, identifying the causes of failure of each barrier. These have been supplemented by available industry data on in-flight engine shut-downs, and SDR data on engine failures [1].

#### **7.5 Engine Failure Fault Tree**

Figure 7.2 shows the quantified version of the ESD for engine failure, taken from the NLR report [1]. This is the starting point for the fault tree development.



## 8. CONSEQUENCE MODELLING

### 8.1 Requirement

In order to show the overall importance of causal factors to accident risks, the CATS model must be able to combine the results of the different ESDs into a suitable risk measure. This should take account of the consequences of each accident from each ESD. The consequence model must provide fatality and damage distributions, capable of being combined with the frequencies of accidents for each ESD to give an overall risk measure.

### 8.2 Consequence Types

Aircraft accidents may result in diverse consequences, including injuries and fatalities to people, damage to property, disruption to business and impacts on the environment. The dominant effects are fatalities to people on-board and damage to the aircraft itself. These are therefore represented in the consequence model. In future work, it would be possible to add other consequence types, such as injuries, external (third-party) fatalities, and costs of delay and disruption resulting from accidents.

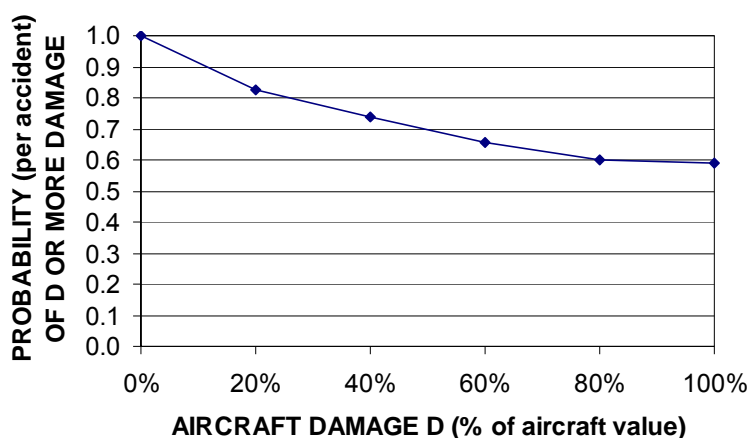
### 8.3 Aircraft Damage Profile

Aircraft damage profiles have been supplied by NLR for each accident from each ESD [16]. These consist of distributions of insurance loss as a percentage of the aircraft hull value. They are based on the insurance loss recorded by Airclaims for accidents that were used to quantify the ESD.

In order to be able to combine the damage from different ESDs, the profiles have been converted to exceedence probabilities for standard damage fractions of 20%, 40%, 80% and 100% of aircraft value. These can be combined after weighting the profile for each ESD by its accident frequency.

Figure 8.1 shows the overall damage profile for all modelled events (excluding ground collisions, ESD 36, for which damage profiles have not yet been obtained). The shape of the curve reflects the fact that most insurance policies treat the aircraft as a total loss (100%) if the repair cost exceeds 75% of the hull value.

**Figure 8.1 Overall Aircraft Damage Profile**



## 8.4 Fatal Accident Probability

Fatalities only occur on a sub-set of accidents. The metric of “fatal accident probability” shows the relative severity of ESD end events. It is the conditional probability that an event will result in one or more fatalities.

Fatality consequences have been obtained from an analysis of fatal accidents in the ADREP database for Western commercial aircraft during 1990-2006. From a dataset of 327 accidents with fatalities on-board that can be represented by the ESDs in the CATS model, a generic fatal accident probability of 0.22 is obtained. In other words, 22% of accidents represented in the ESDs involve one or more fatalities.

In order to estimate this probability for each ESD end event, three alternative methods have been used [10]:

- A. Where the ADREP database includes at least one fatal accident represented by the ESD end event, the probability is obtained from this experience and this ESD alone.
- B. Where the ADREP database has no accidents corresponding to the ESD end event, but there are accidents in the same end state of other ESDs, the probability is obtained from this combined experience.
- C. Where the ESD quantification has used a dataset that does not match the period 1990-2006 used in the analysis of the ADREP database, the probability is obtained from a suitable alternative source in which fatal and non-fatal accidents are known.

These approaches give a fatal accident probability for each ESD end event, even in cases where there is no fatal accident experience. The results are given in full in the DNV consequence model report [10].

## 8.5 Fatal Accident Frequency

The metric of “fatal accident frequency” shows the fatality risk from ESD end events. It is the frequency per flight of accidents involving one or more fatalities.

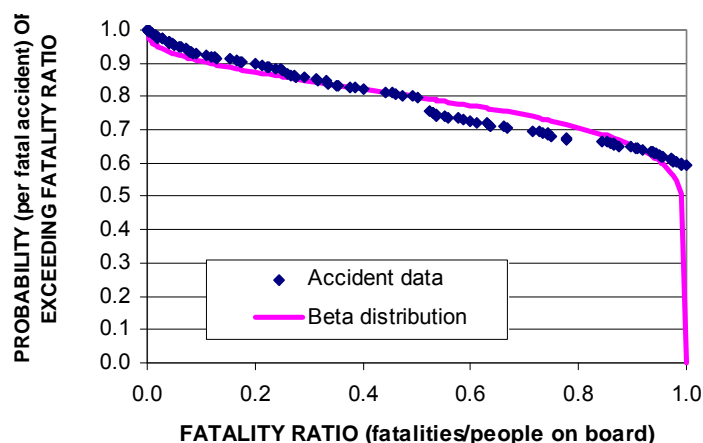
The overall fatal accident frequency estimated by combining the consequence model with the ESDs is  $5.6 \times 10^{-7}$  per flight. This is a preliminary estimate, as a full uncertainty distribution will be determined from the giant BBN model.

Figure 8.2 shows the breakdown for each ESD. It shows that risks are dominated by engine failure and unstable approach. The relatively low contribution from CFIT results from the assumption that all commercial aircraft are fitted with TAWS. This illustrates a prediction that can be made by the CATS model, but which is not available from accident data.

Compared to Figure 2.1, the proportion of fatal accidents due to collisions is high, while the proportion due to structural accidents is low. These suggest opportunities for validation in future work.



**Figure 8.3 Overall On-Board Fatality Profile**



In order to allow the fatality profile to be modified in a consistent way, it is represented by a Beta distribution. In future work, it would be desirable to improve the fit in the region of 100% fatalities.

There are insufficient fatal accidents to obtain a fatality profile for each ESD end event. Therefore, the fatality profile is obtained for the following accident types [10]:

- CFIT (Controlled Flight into Terrain) – ESD 35
- Collision (Mid-Air Collision and Runway Collision) - ESD 2, 31, 32
- Fire ( Fire on Board) – ESD 11
- LOCF (Loss of Control in Flight) – ESD 12 – 16, 18
- LOCL (Loss of Control in Landing) – ESD 19, 21, 23, 25 - 30
- LOCT (Loss of Control in Take-off) – ESD 1, 3-10
- Structural (Structural Damage) – ESD 17, 33

These profiles can then be modified to represent each end event type. The modified distribution is selected so that its expectation value reflects the FR in the accident data for the end event type, while its standard deviation responds to this modification in a way that is characteristic of the accident type. The parameters of the Beta distribution are determined from this. The result is an on-board fatality profile for each ESD end event that is a smooth and consistent adjustment of the data for each accident type. The method is explained in more detail in the consequence model report [10].

The fatality profiles for each end event of each ESD can then be weighted by the fatal accident frequencies and cumulated to give the overall fatality profile. This can be combined with the POB to give the overall FN curve. In future work, it would be preferable to use a distribution for POB to represent the variability more fully.

## 8.7 Consequence Factor Model

The analytical fatality profile above allows the FN curve to be modified in response to influences on the accident consequences. These influences have been identified in the consequence model report [10]. As with the influences on the accident frequencies above, modelling of the dependencies between these consequence factors is challenging and can be addressed in future work. The consequence model report [10] includes simple analyses of the effects of independent factors, and a preliminary model of combined factors.

Quantification of the influences of these factors is based directly on analysis of 327 fatal accidents that can be allocated to ESDs. However, it should be noted that most aircraft accident investigations do not analyse consequence factors in detail, and so data interpretation uncertainty is large at present.

## 8.8 Overall Accident Costs

A metric of “accident cost” combines the overall damage and fatality risk from ESD end events, in the form of the expected accident cost per flight. Other cost types can be added at this stage.

Table 8.1 shows cost estimates of average costs for commercial aircraft supplied by NLR based on the ASICBA project [16]. These include an average aircraft value of €70 million; an average of 9 crew and 85 passengers on board, an average of 0.3 third party fatalities per accident, and a value of preventing a statistical fatality of €2.5 million. In future work, it would be desirable to use probability distributions for these parameters to represent the variability more fully.

**Table 8.1 Average Accident Costs**

HEADS OF COST	COSTS
1. Aircraft physical damage	= % aircraft damage × average insurance value = % aircraft damage × € 70.6 million
2. Possible loss of resale value	if % aircraft damage >= 75% costs = 0 if % aircraft damage < 75% costs = € 7.06 million.
3. Aircraft loss of use	= % aircraft damage × € 4.4 million
4. Aircraft loss of investment return	= 0 (already taken into account)
5. Passenger and crew deaths and/or serious injuries	=% occupant fatalities × (85.2 + 9) × € 2.5 million
6. Site contamination and clearance	= € 1.64 million (for all accident end states)
7. Airline costs for delay	= 0
8. Airport closure	Collision on runway € 41.9 million Runway overrun € 4.4 million Runway veeroff € 4.4 million Aircraft hard landing on runway € 0.5 million
9. Loss of staff investment	= % occupant fatalities × number of crew (= 9) × € 65,000
10. Loss of cargo and/or mail and/or passenger baggage	= % aircraft damage × ( € 94,500 + € 88,693)
11. Search and rescue and cost of emergency services	= € 0.6 million × % aircraft damage.
12. Airline immediate response	= € 3 million × % occupant fatalities
13. Cost of accident investigation	= € 2.5 million × % aircraft damage
14. Third party damage	= 0.3 × € 2.5 million (for all accident end states)
15. Loss of airline income/value/reputation	= 0
16. Social costs	= 0
17. Emergency inspections	= 0
18. Fines, punitive damages, criminal proceedings	= 0

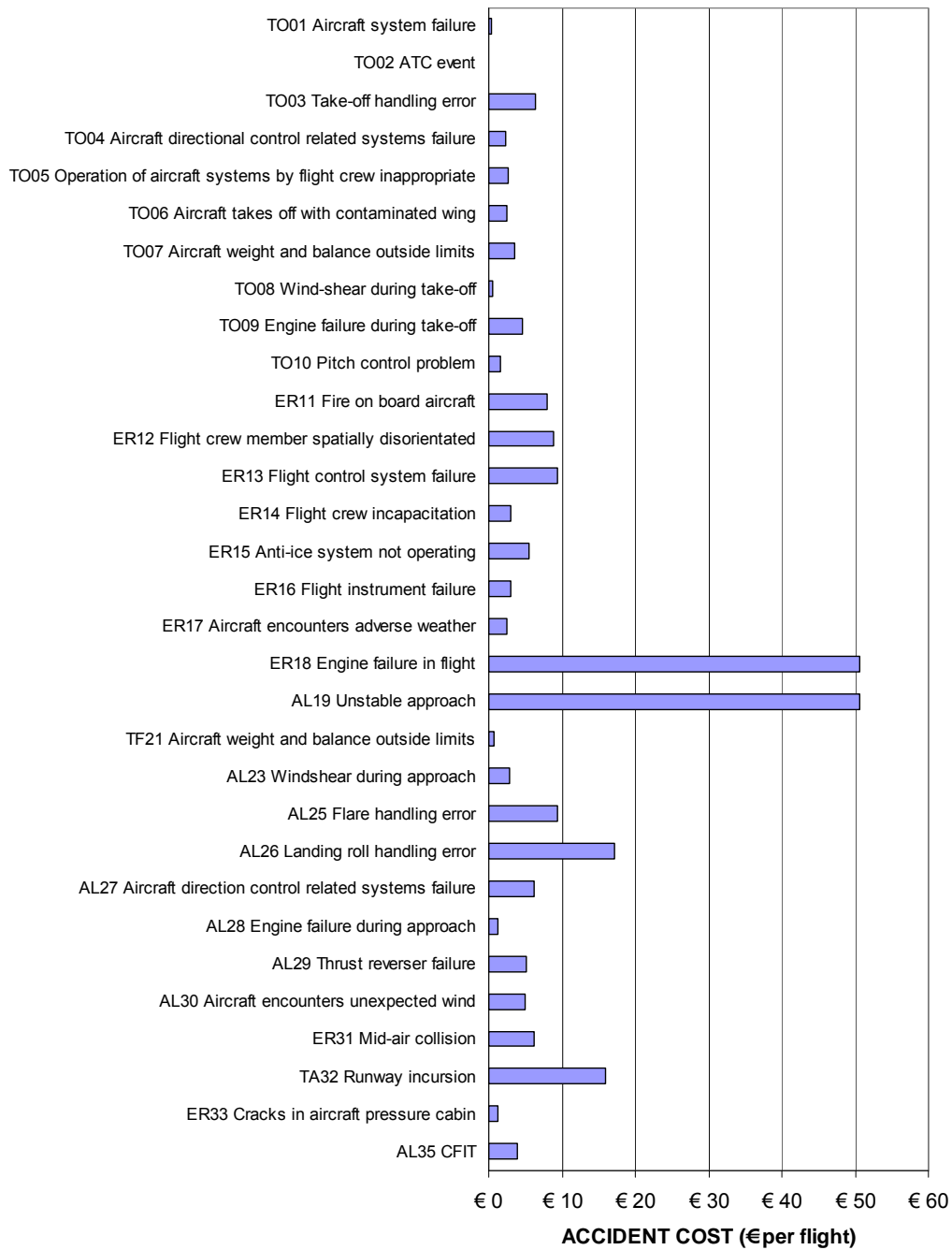
These are combined with the average damage fraction (from Section 8.3) and the average on-board fatality ratio (from Section 8.6), to obtain the expected total cost of each ESD end state.

The average accident cost estimated from the consequence model with the inputs above is €8.0 million per accident, which is an average cost of €240 per flight when spread over all commercial flights world-wide. This is a preliminary estimate, as above, and excludes ground collision, whose costs have not yet been accurately estimated. The breakdown by cost type is:

- 59% from physical damage to the aircraft
- 38% from on-board fatalities
- 4% from airport closure
- 10% from other modelled components

Figure 8.4 shows the results for each ESD. It shows that accident costs are dominated by engine failure and unstable approach with a relatively low contribution from CFIT results as above. It would be desirable to include ground collision in future work. This illustrates the type of information that could be used as an input to cost-benefit analysis of risk reduction measures.

**Figure 8.4 Accident Cost Results**



## 9. REFERENCES

1. NLR, "Quantification of Event Sequence Diagrams for a Causal Risk Model of Commercial Air Transport", NLR-CR-2006-520, October 2006.
2. DNV, "Controlled Flight into Terrain Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/1, Rev2, June 2008.
3. DNV, "Loss of Control in Flight Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/4, Rev1, 20 October 2006.
4. DNV, "Loss of Control on Landing Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/5, Rev1, 27 June 2006.
5. DNV, "Loss of Control on Take-Off Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/6, Rev0, 20 October 2006.
6. DNV, "Engine Failure in Flight Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/7, Rev0, 17 July 2007.
7. DNV, "Structural Failure in Flight Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/8, Rev0, 17 July 2007.
8. DNV, "Fire in Flight Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/9, Rev0, 17 July 2007.
9. DNV, "Mid-Air, Runway & Ground Collision Fault Tree Model", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/10, Rev1, June 2008.
10. DNV, "Consequence Model for Aircraft Accidents", Report for Ministerie van Verkeer en Waterstaat, DNV Project C21004587/11, Rev0, June 2008.
11. EUROCONTROL, "Main Report for the 2005/2012 Integrated Risk Picture for Air Traffic Management in Europe", EEC Note 05/06, March 2006.
12. NASA Office of Safety and Mission Assurance, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", August 2002
13. Mosleh, A. et al (1997), "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment", NUREG/CR-5485
14. Boeing, "Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations, 1959-2003", Boeing Commercial Airplanes Group, Seattle, WA, USA (updated annually).
15. Bateman, D. (2003), "How to Terrain-Proof the World's Civil Aircraft Fleet", IASS.
16. NLR, "Aircraft Damage and Occupant Fatality Profiles for a Causal Risk Model of Air Transport Safety", NLR-CR-2008-231, May 2008.
17. NLR, "A Method for Assessing Safety Improving Measures", Aviation Safety Improvement Using Cost-Benefit Analysis (ASICBA) project report NLR-WP3-D31, October 2006.

## 10. ACRONYMS

ACAS	airborne collision and avoidance system
ADI	attitude director indicator
ADREP	Accident/Incident Data Reporting
AL	approach and landing
ATC	air traffic control
BBN	Bayesian Belief Network
CATS	Causal model of Air Transport Safety
CFIT	controlled flight into terrain
CL	climb
DME	distance measuring equipment
DNV	Det Norske Veritas
ER	en route
ESD	event sequence diagram
FMS	flight management system
FN	frequency-number of fatalities
FOD	foreign object debris
FT	fault tree
FR	fatality ratio
GPWS	ground proximity warning system
ICAO	International Civil Aviation Organization
IMC	instrument meteorological conditions
IRP	integrated risk picture
LLWAS	low-level wind-shear alert system
LOC	loss of control
LOCF	loss of control in flight
LOCL	loss of control in landing
LOCT	loss of control in take-off
MF	modification factor
MSAW	minimum safe altitude warning system
MTOW	maximum take-off weight
NLR	National Aerospace Laboratory
PF	pilot flying
PNF	pilot not flying
PWS	predictive wind-shear
RIMCAS	runway incursion monitoring and collision avoidance system
RR	risk ratio
SDR	Service Difficulty Reports
TAWS	terrain awareness & warning system
TMA	terminal manoeuvring area
TO	take-off
VHF	very high frequency
VOR	VHF omni-directional radio range