



Executive summary

Accident scenarios for an integrated aviation safety model

Problem area

An essential element of safety management is a system to achieve safety oversight. FAA is moving towards a Systems Approach for Safety Oversight (SASO). In support of the SASO program, FAA has initiated research requirements, including a requirement to develop a methodology to identify hazards and assess risks within the 14CFR Part 121 aviation system. To meet requirement CA-02, University of Maryland, Hi-Tec Systems and the National Aerospace Laboratory NLR are jointly developing an integrated risk model. The proposed risk model architecture introduces a hybrid causal model of Event Sequence Diagrams, Fault Trees and Bayesian Belief Networks.

The objective of the current study is to develop generic accident scenarios that form the upper layer of the integrated risk model.

Description

Main accident types have been defined based on the ICAO definition of an accident, in order to systematically develop accident scenarios: abrupt maneuver, cabin environment, uncontrolled collision with ground, controlled flight into terrain, forced landing, mid-air collision, collision on ground,

structure overload and fire/explosion. The accident scenarios are grouped by accident type and different flight phases. The Event Sequence Diagram (ESD) methodology is used for representing accident scenarios.

Results

36 generic accident scenarios have been modelled in the current study based on a combination of retrospective analyses and prospective analyses. These scenarios describe qualitatively the sequence of events at a high level of abstraction. The high level of abstraction is required to make the scenarios easy to understand for users and to keep the model transparent and simple at the top layer of the integrated risk model. Complexity and details will be added (later) in the underlying sub-models.

Conclusions

The Event Sequence Diagram methodology is an appropriate technique for modeling accident scenarios for the purpose of the SASO program. Criteria have been established for the selection of initiating and pivotal events.

Report no.

NLR-CR-2005-560

Author(s)

A.L.C. Roelen and R. Wever

Classification report

Unclassified

Date

November 2005

Knowledge area(s)

Safety
Aircraft operations

Descriptor(s)

causal model, event sequence diagram, accident scenarios

Recommendations

A next step in the model development should be the quantification of the ESDs, which is necessary to enable their use in accident risk assessments.

An essential step in order to expand the integrated risk model is to develop the first layer of the fault trees under the ESDs. The first layer of the fault trees will further clarify the causal pathways towards initiating and pivotal events in the accident scenarios.



NLR-CR-2005-560

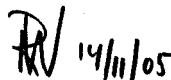

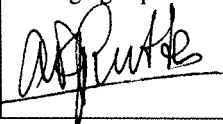
Accident scenarios for an integrated aviation safety model

A.L.C. Roelen and R. Wever

No part of this report may be reproduced and/or disclosed, in any form or by any means without the prior written permission of the owner.

Customer: FAA/IVW
Contract number: 404.38.330
Owner: FAA/IVW
Division: Air Transport
Distribution: Limited
Classification title: Unclassified
November 2005

Approved by:

| | | |
|---|---|--|
| Author  14/11/05 | Reviewer  14/11/05 | Managing department  15/11/05 |
|---|---|--|



Summary

An essential element of safety management is a system to achieve safety oversight. FAA is moving towards a Systems Approach for Safety Oversight (SASO). In support of the SASO program, FAA has initiated research requirements, including a requirement to develop a methodology to identify hazards and assess risks within the 14CFR Part 121 aviation system (Requirement Number CA- 02 *Hazard Identification and Risk Analysis for 14CFR Part 121*). To meet requirement CA-02, University of Maryland, Hi-Tec Systems and the National Aerospace Laboratory NLR are jointly developing an integrated risk model. The proposed risk model architecture introduces a hybrid causal model of Event Sequence Diagrams, Fault Trees and Bayesian Belief Networks.

The objective of this study conducted by NLR is the development of generic accident scenarios that are at the upper layer of the integrated safety model. The scenarios describe the combination of events or conditions including the sequence of their occurrence that results in the transition of a hazard to an accident. It was concluded that the Event Sequence Diagram methodology is appropriate for modeling accidents scenarios.

Criteria have been established for the selection of initiating and pivotal events. In order to systematically develop accident scenarios this study defined main types of accidents for the integrated safety model based on the ICAO definition of accident: abrupt maneuver, cabin environment, uncontrolled collision with ground, controlled flight into terrain, forced landing, mid-air collision, collision on ground, structure overload and fire/explosion. Accident scenarios are grouped by accident type and different flight phases. Subsequently, generic accident scenarios have been modeled through a combination of retrospective and prospective analysis. The result is a set of 36 event sequence diagrams. The developed scenarios describe qualitatively at a high level of abstraction the sequence of events in different accident type / flight phase combinations. The high level of abstraction is required to make the scenarios easy to understand for users and to keep the model transparent and simple at the top layer of the integrated risk model. Complexity and details will be added (later) in the underlying submodels.

The study recommends the quantification of the developed ESDs to enable the use of the ESDs in accident risk assessment. Furthermore, it is recommended to develop the first layer of the fault trees underlying the initiating and pivotal events in the scenarios. This is an essential step in expanding the integrated safety model. The first layer of the fault trees will further clarify and define the causal pathways to the initiating and pivotal events in the scenarios.



Contents

| | |
|--|-----------|
| List of abbreviations | 6 |
| 1 Introduction | 7 |
| 1.1 Background | 7 |
| 1.2 Research objective | 9 |
| 1.3 Research challenges | 9 |
| 1.4 Acknowledgements | 9 |
| 2 Experience from other industries on the use of accident scenarios for risk modeling | 10 |
| 2.1 Nuclear industry | 10 |
| 2.2 Experience from the aerospace industry | 10 |
| 2.2.1 Aircraft certification | 10 |
| 2.2.2 Spaceflight | 11 |
| 2.2.3 Air Traffic Management | 11 |
| 3 Model application and user requirements | 13 |
| 3.1 Introduction | 13 |
| 3.2 Potential users | 13 |
| 3.3 User objectives | 13 |
| 3.4 Compatibility with Reason's model | 15 |
| 3.5 Proposed approach | 17 |
| 3.6 Dynamics | 18 |
| 4 Scenario clustering | 19 |
| 4.1 Accident type | 19 |
| 4.2 Flight phase | 22 |
| 5 Event Sequence Diagram | 25 |
| 5.1 General theory | 25 |
| 5.2 Criteria for selecting initiating events | 27 |
| 5.3 Criteria for selecting pivotal events | 28 |
| 5.4 End state | 29 |



| | | |
|-------------------|---|-----------|
| 6 | Scenario development | 30 |
| 6.1 | ESD development steps | 30 |
| 6.2 | Retrospective and prospective analysis | 30 |
| 6.3 | Definitions of initiating and pivotal events | 31 |
| 6.4 | Existing definitions and taxonomies | 32 |
| 6.5 | Results | 33 |
| 6.6 | Example of hybrid logic | 35 |
| 7 | Discussion | 36 |
| 8 | Conclusions and recommendations | 37 |
| 8.1 | Conclusions | 37 |
| 8.2 | Recommendations | 37 |
| 9 | References | 38 |
| Appendix A | List of accidents used for the development of ESDs | 41 |
| Appendix B | Event sequence diagrams | 45 |
| Appendix C | Accident classification taxonomies | 65 |
| Appendix D | ICAO accident definition | 67 |

(70 pages in total)



List of abbreviations

| | |
|-------|---|
| ATC | Air Traffic Control |
| ATM | Air Traffic Management |
| CAP | Civil Aviation Publication |
| CAST | Commercial Aviation Safety Team |
| CFIT | Controlled Flight Into Terrain |
| ESARR | Eurocontrol Safety Regulatory Requirement |
| ESD | Event Sequence Diagram |
| FAA | Federal Aviation Administration |
| ICAO | International Civil Aviation Organization |
| JSAT | Joint safety Analysis Team |
| NRC | Nuclear Regulatory Commission |
| NTSB | National Transportation Safety Board |
| PRA | Probabilistic Risk Assessment |
| QRAS | Quantitative Risk Assessment System |
| SASO | Systems Approach to Safety Oversight |



1 Introduction

1.1 Background

A safe aviation system is a vital element of modern society. Achieving excellent aviation safety levels requires a concerted international and national action by many actors, including systematic management of the risks associated with flight operations and related activities to achieve high levels of safety performance [CAP 712].

An essential element of safety management is a system to achieve safety oversight. FAA is moving towards a Systems Approach for Safety Oversight (SASO) where System Safety is 'The application of engineering and management principles, criteria, and techniques to reducing accidents and incidents'. In support of the SASO program, FAA has initiated research requirements, including Requirement Number CA- 02 *Hazard Identification and Risk Analysis for 14CFR Part 121*. This requirement is defined as follows:

General Requirement

A methodology shall be developed to identify hazards and assess risks within the 14CFR Part 121 aviation system. The methodology shall be validated by using it to identify and analyze a subset of hazards and risks within the 14CFR Part 121 aviation system.

Specific Requirements

At a minimum, hazards in the aviation system shall be identified in the area of operational functions and procedures. Hazards and risks in other areas of the aviation system such as aircraft and equipment malfunctions, hazards due to organizational set-up (structure, policy, culture), human errors, environmental hazards (wind, turbulence, terrain), and contributory hazards (regulatory, system, economy) shall be identified as time permits. The hazard identification and risk analysis shall produce at a minimum: 1) a comprehensive classification that covers all potential hazards involved in air carrier operations, 2) a list of potential hazards for the classes that fall within the scope of this project, and 3) a probabilistic method to evaluate risk. The study shall use, but is not necessarily limited to, the ACOSM CFR Part 121 aviation system model, accident/incident reports, relevant technical papers, and the opinions of subject matter experts. A hazard coding system shall be developed.

To meet requirement CA-02, University of Maryland, Hi-Tec Systems and the National Aerospace Laboratory NLR are jointly developing an integrated risk model. A similar effort, initiated by the Dutch Ministry of Transport, has started in the Netherlands. Frequent exchange



of information between the two projects is aimed at a common model framework and avoiding duplication of work.

The requirement for completeness (system wide) and the potential complexity of the integrated risk model lead to the development of a hierarchical model architecture. The proposed risk model architecture [Mosleh et al 2004] is displayed in Figure 1. The proposed methodology extends the conventional risk analysis techniques, e.g. fault trees and event trees by introducing a hybrid causal model of event sequence diagrams, fault trees and influence diagrams. Event Sequence Diagrams (ESDs) are used to define the context within which various causal factors would be viewed as a hazard. A context can be a combination of events or conditions including the timeline of their occurrence that results in the transition of a hazard to an accident. A context can be described as an accident scenario.

The enumeration of the causes of the ESD initiators and intermediate events is done through hybrid logic. The term ‘hybrid logic’ is used to indicate that deterministic causes such as direct hardware and software failure events are handled by Fault Tree logic gates, while probabilistic causal relations such as the impact of organizational factors are treated with influence diagrams or Bayesian Belief Nets.

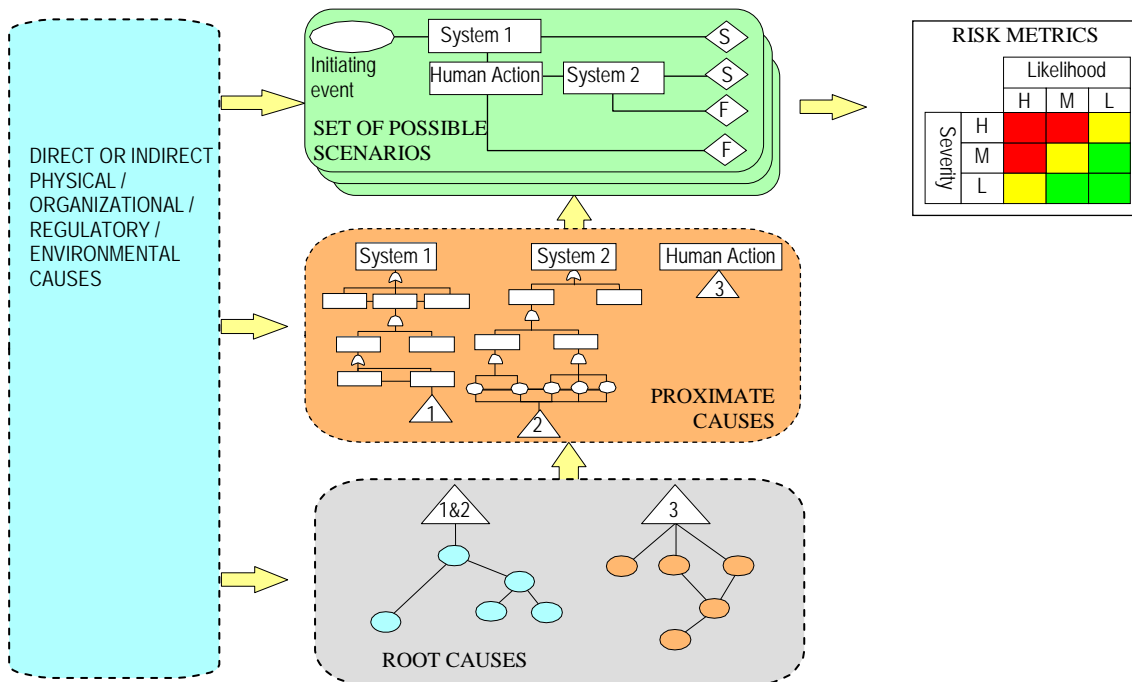


Figure 1: Integrated Safety Model framework showing the Event Sequence Diagrams at the top, Fault Trees in the middle and the influence diagrams at the bottom.



1.2 Research objective

The objective of this task is the development of generic accident scenarios that are at the upper layer of the integrated safety model shown in Figure 1. This task will analyze different possible ways to describe scenarios, and will select the most appropriate, i.e. most suitable for this modeling effort.

1.3 Research challenges

By scenario, we mean a sequence of events, which ‘starts’ with some event and ‘ends’ in another. These start and end points are somewhat arbitrary and depend on the objectives of the analysis. While the description of accident scenarios may seem to be a trivial task, the decisions that are implicitly or explicitly made in this description may have far reaching consequences for the integrated risk model as a whole. Because of the far reaching consequences of the selection and definition of the accident scenarios, it is essential that this is done carefully. Proper definition of accident scenarios can reduce the overall development effort and can help in creating more or less independent submodels that can be developed separately. It is therefore particularly important to have a clear overview of the different possible ways of describing scenarios and the impact that these different methods may have on overall causal model development and the use of the model. To be able to select the most appropriate method, it is necessary to compare these impacts against the objective and expected use of the causal risk model.

Together these generic accident scenarios form a part of the overall risk model that is the most straightforward to understand for non-modeling specialists, including potential users of the model. The face validity of the accident scenarios is one of the characteristics that will determine overall confidence in the integrated risk model. It is therefore essential that a range of potential users of the integrated risk model broadly endorse the generic accident scenarios.

Another difficulty is that it is extremely challenging to identify comprehensively all significant scenarios [Stamatelatos et al. 2002].

1.4 Acknowledgements

The authors are in debt to Tommy McFall, Richard C. Berg and Harold Donner of FJLeonelli Group for their critical review. We would like to thank Ali Mosleh (University of Maryland) for providing comments and ideas for this research. Many thanks also to Jennelle Derrickson (FAA Tech Center) and Hok Goei (CAA the Netherlands) for the overall monitoring and coordination. All results and conclusions are the authors’ and not necessarily endorsed by the consulted persons.



2 Experience from other industries on the use of accident scenarios for risk modeling

The idea of using accident scenarios as a tool for risk analysis is in itself not new or innovative. Risk modeling as part of a structured approach to risk assessment and mitigation has been applied in the past in different industries. This section provides an overview of some of the more relevant developments and experiences on the use of accident scenarios for risk modeling.

2.1 Nuclear industry

The desire to quantify and to evaluate the effects of design improvements of nuclear powerplants led to the introduction of Probabilistic Risk Assessment (PRA) in the nuclear industry. The methods of Probabilistic Risk Assessment originated from the aerospace industry in the 1960s. The first full-scale application of these methods to a commercial powerplant was undertaken in the Reactor Safety Study WASH-1400 published by the American Nuclear Regulatory Commission NRC in 1975 [NRC 1975]. Earlier design assessments simply looked at system reliability (success probability), given a design basis challenge. The review of nuclear plant license applications did essentially this, culminating in findings that specific complements of safety systems were single-failure proof for selected design basis events. Going well beyond this, WASH-1400 modeled scenarios leading to large radiological releases from commercial nuclear powerplants. It considered highly complex scenarios involving success and failure of many and diverse systems within a given scenario, as well as operator actions and phenomenological events. These kinds of considerations were not typical of classical reliability evaluations [Stamatelatos et al. 2002]. While this report was controversial, independent evaluation of the study [Lewis et al. 1979] led to recommendations for improvement. The Three Mile Island accident in 1979 and subsequent accident investigation underlined the value of Probabilistic Risk Assessment [Kemeny 1979]. When the PRA procedures guide [NRC 1983] was published by the NRC in 1983 it became a main reference. PRA became even more accepted when in 1995 the NRC issued a revised policy statement on the use of PRA, which stated that “The use of PRA technology should be increased in all regulatory matters” [NRC 1995].

2.2 Experience from the aerospace industry

2.2.1 Aircraft certification

In the aviation industry, the increased complexity of systems and in particular the development of automatic landing systems in the 1960s led to a need to examine the effects of combinations of failures, and a need to consider the likelihood of occurrence of failures [Lloyd & Tye 1982]. Certification requirements for aircraft system design and analysis were updated to include a



requirement to conduct structured safety analysis or assessment at the aircraft level. The required depth of the analysis depends on the types of functions performed by the system, the severity of the failure conditions and whether or not the system is complex. For less severe failure conditions, experienced engineering and operational judgement may be used, while for hazardous or catastrophic failure conditions, a very thorough safety assessment is necessary. Among accepted techniques for safety assessments are Design Appraisal, Installation Appraisal, Failure Modes and Effects Analysis, Fault Tree or Dependence Diagram Analysis and Markov Analysis [JAA, AMJ 25. System Design and Analysis].

2.2.2 Spaceflight

In the same time period that saw the development of PRA in aircraft development, the US manned space program, and in particular the Apollo missions to the surface of the moon and back, led to the advancement of PRA at NASA. Apollo program estimates of mission success were very low and unacceptable as risk levels to be incurred during an actual mission. However, of the seven Apollo missions between 1969 and 1972, only one (Apollo 13) was a (non catastrophic) failure. The discrepancy between the apparent high mission success rate and the earlier estimates caused dissatisfaction with PRA at NASA. Instead, qualitative methods based on Failures Modes and Effects Analysis (FMEA) were used [Fragola]. It was only after the accident with the Space Shuttle Challenger in 1986 and the subsequent accident investigation report [Rogers 1986] that PRA was re-introduced at NASA. Under contract to Marshall Space Flight Center, the University of Maryland developed software for a Quantitative Risk Assessment System (QRAS). Risk modeling within QRAS is done by a combination of Event Sequence Diagrams and Fault Trees.

2.2.3 Air Traffic Management

Eurocontrol Safety Regulatory Requirement (ESARR) 4 'Risk Assessment and Mitigation in ATM' concerns the use of a quantitative risk-based approach in Air Traffic Management when introducing and/or planning changes to the ATM system. This requirement covers the human, procedural and equipment (hardware, software) elements of the ATM System as well as its environment of operations. The requirement is consistent with amendment 40 to ICAO Annex 11, mandating the use of safety assessment of significant changes in the air traffic system.

ESARR 4 specifies the maximum tolerable probability of ATM directly contributing to an accident is $1.55 * 10^{-8}$ per flight hour, or $2.31 * 10^{-8}$ accidents per flight. Professional judgment was used to determine the maximum acceptable ATM direct contribution to accidents and 20 years of historic data were selected to confirm the credibility of this target.



The explanatory material on ESARR 4 requirements states [EUROCONTROL 2003]: “The feasibility of setting quantitative objectives / targets for specific parts of the ATM system was discussed, especially when it comes to their allocation to human contributions, procedures and software. It is recognized that demonstration of compliance won’t always be quantitative – based, as it does not seem feasible to demonstrate a priori and in a quantified manner that a good working process, such as training, Safety Management System, or software codes of practices, enable specific quantitative objectives to be met. This will only be based on professional judgment and potentially verified over time.”

The increasing integration, automation and complexity of the ATM system requires a systematic and structured approach to risk assessment and mitigation, including hazard identification, as well as the use of predictive and monitoring techniques to assist in these processes [EUROCONTROL 2003].

ESARR explanatory material recognizes that a combination of quantitative (e.g. mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgment) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met.

The explanatory material emphasizes the development of safety monitoring and data collection mechanisms. The rationale is that any model (e.g. Collision Risk Model) used in risk assessment must be validated, and real data could contribute significantly to this validation process.



3 Model application and user requirements

3.1 Introduction

Causal risk modeling is a powerful tool in supporting the insight into the interdependencies between the constituent parts of complex systems. As far as safety is concerned the propagation of fault situations can be modeled and followed. Weaknesses in protection against fault propagation can systematically be determined. The power of causal risk modeling can be greatly enhanced if probabilities and logical dependencies can be quantified. The effect of safety measures or conversely the breach of safety barriers then can be evaluated quantitatively allowing comparisons between alternative safety measures and cost benefit considerations. Such a causal risk model is a proper tool for Probabilistic Risk Assessment. It can be used for proactive safety management.

3.2 Potential users

The potential users of a causal risk model are both the regulator/authorities and industry. Governmental use of the model includes assisting both safety policy development and safety oversight. The industry includes airport organizations, airlines and the air navigation service providers.

3.3 User objectives

The proposed integrated methodology is intended to address multiple requirements and practical needs [Mosleh et al 2004, Dutch project group causal modeling 2003]:

- Identify safety hazards, including those rooted in the system and its (internal and external) physical, human, organizational, and regulatory environment.
- Ranking hazards, the ability to provide a quantitative relative importance of the identified hazards,
- Supporting risk-informed decision making on matters of safety significance,
- Evaluating safety significance of abnormal conditions, failures and incidents.
- To help clarify the effect of technical, operational and managerial factors on the accident risks.
- To help direct risk reduction effort towards areas where it will be most effective.
- To help explain the reasons for actions on improving air safety.
- To provide improved estimates of accident risks.



Primary uses envisioned are [Mosleh et al 2004]:

- Understanding hazards and their cause-effect relationship,
- A quantitative risk analysis platform for supporting risk-informed decision-making, and in developing auditing tools, risk indicators & performance measures, diagnosis tools, strategic plans, and creation/removal of aviation regulations and guidance material such as Advisory Circulars (AC). Another extremely important role that a model-based approach for above objectives can play is as a common language between aviation safety R&D, industry, and regulatory entities on issues of safety.
- An environment for model-based inspection, event analysis, data gathering and analysis, and accident precursor analysis.

The user objectives of a causal risk model, as listed in the final report of the Dutch project group causal modeling¹, are the following [Dutch project group causal modeling, 2003]:

- The ability to make comparative judgment:
 - With other modes of transport
 - In time
 - Between different airports
 - Between individual elements of the safety system.
- Ability to diagnose the risk situation within the own organization and across its borders, in order to pro-actively improve aviation safety.
- Ability to set priorities within the whole set of possible safety measures (e.g. based on an assessment of the efficiency of individual measures).
- Surveillance of the safety quality provided by the aviation system and its individual elements.
- Informing the public on safety policy and safety efforts.

The requirement to be able to use the model to clarify and explain the reasons for safety measures is particularly important for this research task. To meet this requirement, the generic accident scenarios must be kept as simple as possible and must be easy to understand. They must describe accidents in such a way that people agree that it is useful and are comfortable with it.

¹ This group consisted of representatives from the Ministry of Transport, Schiphol airport, Air Traffic Control the Netherlands and KLM.



3.4 Compatibility with Reason's model

For people to be comfortable with the model requires that it must be in agreement with (internationally) accepted concepts, models and methods. One of the best known and most used concepts is what is often referred to as the Reason 'model', see Figure 2 [Reason 1990].

Reason's theory of accidents recognizes two types of failures:

- Active failures,
- Latent (or hidden) failures.

Active failures are the unsafe activities that occur right before or during the accident, they involve people making errors and violations. Usually active failures are committed by those on the "front line" of the system: control room personnel, drivers, ship's crews, personnel on the shop floor, flight crew, etc. Latent failures are failures that are created a long time before the accident, but lie dormant until an active failure triggers their operation. Their defining feature is that they were present within the system well before the onset of an accident sequence. Like many other high-hazard, low-risk systems, the aviation system has developed such a high degree of technical and procedural protection that it is largely proof against single failures, either human or mechanical. The aviation system is more likely to suffer 'organizational accidents' [Reason 1990]. That is, a situation in which latent failures, arising mainly at the managerial and organizational level, combine adversely with local triggering events and with the active failures of individuals at the execution level [Reason 1997].

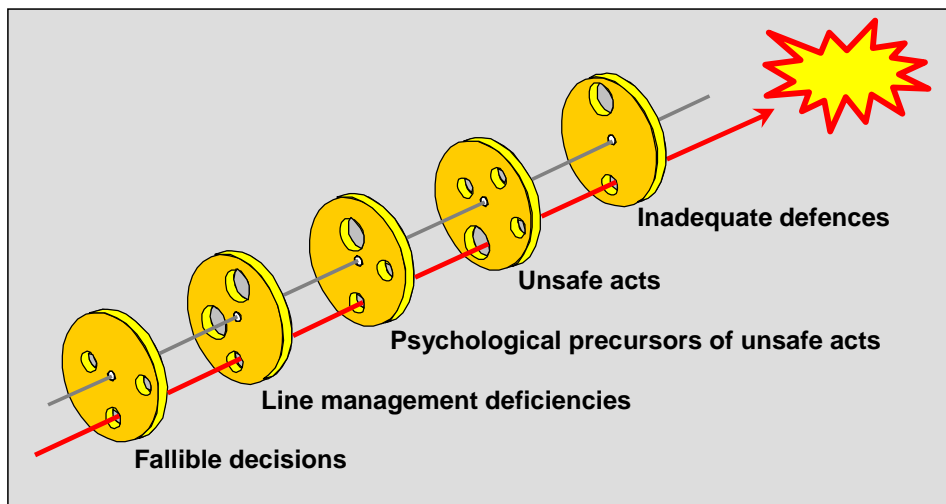


Figure 2: Reason model of accidents.



The pictorial representation of Reason’s model of an accident (Figure 2) suggests independence between the different types of failures that together form an accident. In reality, those failures will be more or less dependent. This will make the modeling more complicated than is suggested in Figure 2.

The notion of active failures and latent failures serves as a useful criterion for deciding which elements of the causal chain should be represented directly in the scenarios. The further the accident sequence is traced back in time, the more the factors revealed penetrate into organizational factors related to management and organization. They are related to issues such as training of competence, supervision, manpower planning to avoid fatigue and task overload, incident analysis for improvement of risk control, inspection and maintenance scheduling to optimize control of hardware failures, etc.

Accident scenarios will be composed of active failures only. Latent failures will be represented in the Fault Trees and Influence Diagrams that constitute the other layers of the integrated safety model framework, see Figure 3. Limiting the scenarios to active failures limits the size of the scenarios and makes them easier to understand. Furthermore, latent failures are often ‘common mode’ and/or ‘soft’ causal relations, which can be better expressed in influence diagrams rather than ESDs. An example of a ‘soft’ relationship is the common mode effect of safety culture on certain events in the scenarios.

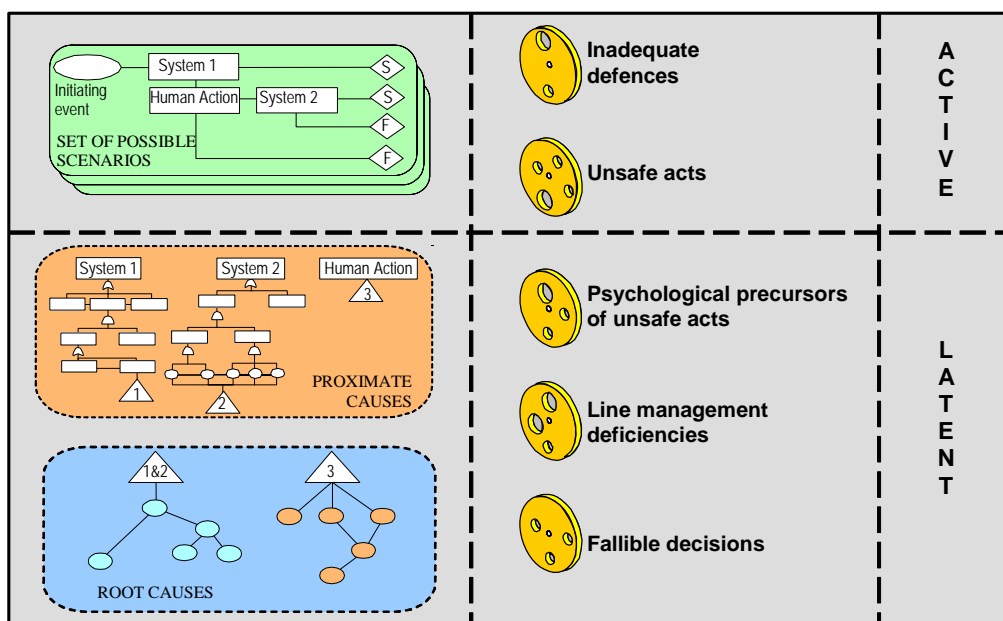


Figure 3: Active failures are represented in the accident scenarios, latent failures are covered by other parts of the model.



3.5 Proposed approach

Which methodology for risk modeling is most suitable for representing accident scenarios depends on how the characteristics of these methods match with the user requirements.

Methodologies that have been successfully applied include the following [Labeau et al 2000]:

- State transition diagrams
- Petri nets
- GO-FLOW
- Dynamic flow graph methodology
- Event Sequence Diagrams (ESDs)

A characteristic of the ESD approach is that it is scenario-based as opposed to other techniques which are component-based [Labeau et al 2000]. An advantage is that the ESDs are self-explanatory; they provide an intuitive understanding of the scenarios. There is explicit representation of sequences, thresholds on process variables and timing of events. We propose to use conventional ESD techniques, primarily because they provide an easy understanding of the scenarios. Basic components are logically combined and temporally ordered to obtain event trees. Mathematically the conventional ESD approach is relatively simple. It only requires elementary knowledge of Boolean algebra and probability theory.

A disadvantage of this methodology is that sequence delineation, including simplifications and compromises which need to be made, has to be performed by the analysts. The burden of proof of correctness of the outcome lies with the analyst, as opposed to other methods where the burden of proof of correctness is shifted from the analyst to the methodology itself [Labeau et al 2000]. Therefore, the quality of the ESD is analyst dependent, which means that the team that develops the ESDs must have in-depth knowledge of the aviation system, with emphasis on flight operations.

The above mentioned characteristics of the ESD approach makes it an appropriate technique for representing accident scenarios for the purposes as required by the SASO program. Therefore this technique has been adopted.



3.6 Dynamics

When the basic characteristics of the system change in time such that the rules, structure, etc., change, the system can be regarded as a *dynamic* system. Some of the dynamics may not necessarily be on time, but on interactions between different components of the system. In these cases the system is said to be *highly coupled*. Dynamic risk assessment methods provide a framework for explicitly capturing the influence of time and process dynamics on scenarios. Despite the potential for greater correctness, these methods have not yet seen such wide application as conventional methods, primarily because of their greater complexity. At this stage of model development it has been decided not to include dynamics in the scenarios. The focus is on creating a broad set of high level scenarios. If at a later stage it is deemed necessary, dynamics can be introduced. ESDs allow posterior introduction of dynamics and are flexible enough to restrict the dynamic analysis to only where it is necessary [Labeau et al 2000].



4 Scenario clustering

There are hundreds or maybe even thousands of possible accident scenarios imaginable. A review of past accidents will not necessarily result in a complete overview of all accidents that are possible, because some potential accident scenarios may not have been realized. A systematic decomposition is required to be able to capture all possible accidents.

While we are not able to describe each individual accident scenario in detail, we must have a way of structuring that allows us to identify groups or classes of scenarios. For each group or class we can then develop a representative generic accident scenario. A structured way of clustering or grouping accident scenarios will help to reduce the overall model development effort. We propose to look at accident type and flight phase as main criteria for clustering accident scenarios. The reasons are explained in the next section.

4.1 Accident type

The ultimate measure of safety is accident probability. Therefore we propose to focus on *accident* scenarios. The term 'accident' is precisely defined in ICAO Annex 13 (refer to Appendix D). Generally, an accident is an occurrence where:

- a) a person has been fatally or seriously injured, or
- b) the aircraft sustains major damage or structural failure.

Categorization of accidents is essential to simplify the modeling. The accident categories should be mutually exclusive, so that their results can be added together and should give complete coverage of all accident risks [Roelen et al 2000]. The accident categorization used in the present study is based on the ICAO definition of an accident. Accident is accordingly further divided into subcategories 'personal injury' (including fatality), 'aircraft destroyed' and 'aircraft damaged'. On a high level of abstraction there are four ways for a person to get fatally or seriously injured, or for an aircraft to be destroyed or sustain major damage or structural failure:

- Personal injury only (without the aircraft being damaged or destroyed)
- Collision of aircraft with the ground
- Collision of aircraft with an object
- General disintegration of aircraft

There can be occurrences in which the aircraft has little or no damage, but the occupants are seriously injured or even killed. Other than security related events, this can happen when there is an abrupt maneuver, e.g. a sudden and unexpected turbulence encounter resulting in passengers thrown around in the cabin, or in case of an event involving the cabin environment, e.g. fire or lack of oxygen.

A collision with the ground can be controlled, when the aircraft has no malfunctions and is under control of the flight crew, albeit that the crew is not aware of the fact that they are flying



towards terrain, i.e. controlled flight into terrain. A collision with the ground can also be uncontrolled, when the flight crew has lost control of the aircraft, which can be induced by the crew, an aircraft system/mechanical malfunction or the environment. Thirdly, collision with ground can also be a forced landing, where the crew makes an unscheduled landing off a runway after they are unable to continue flight.

A collision with an object can be an in-flight collision with another aircraft, or it can be a collision on the ground with another aircraft, a vehicle, or other object. A 'general disintegration' is an occurrence where the aircraft structure is overloaded and damaged, including in-flight disintegration, either due to a structural failure or due to fire or an explosion (e.g. fuel tank explosion or the detonation of a bomb).

The resulting set of accident archetypes is shown in Figure 4. This way of categorizing accidents is generally in agreement with the tradition in aircraft accident statistics (see for instance references CAP 681, CAP 701, and the brochure 'Civil Aviation Safety Data, 1989-2003 from the Transport and Water Inspectorate the Netherlands), although there is no strict convention.

Each of the main accident types can obviously be further subcategorized. However, the distinction between different accident types becomes less clear when we try to further subcategorize. Internal consistency becomes more difficult to maintain. It is more useful to make a different cross section of the total set of possible accidents. We propose to do this by distinguishing between different phases of flight (see section 4.2).

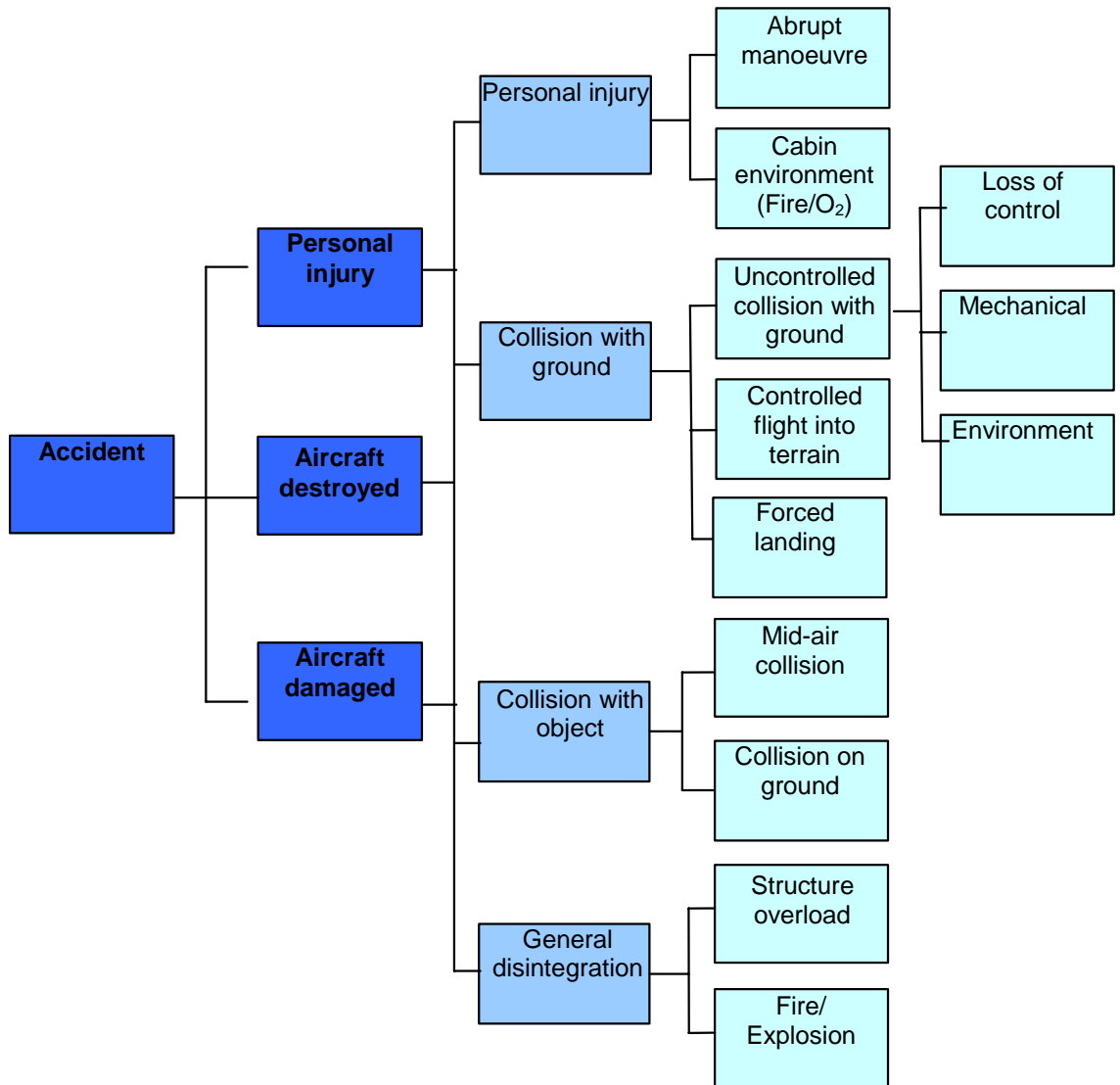


Figure 4: Accident archetypes.

Definitions of each of the accident archetypes have been developed, taking into account existing definitions, in particular the CAST/ICAO Common Taxonomy Team (CICCT) Aviation Occurrence Categories definitions. CICCT definitions of occurrence categories could not be used directly however because these are designed to permit the association of multiple categories within an accident. In our case, we need categories that are mutually exclusive. Accident type definitions are listed in Table 1.



Table 1: Accident type definitions.

| | |
|------------------------------------|---|
| Abrupt maneuver | Abrupt maneuver of the aircraft due to an action by flight crew (intentional or unintentional) or due to external factors such as turbulence or aircraft systems malfunction. |
| Cabin environment | Occurrence involving the condition of the cabin environment leading to occupants fatalities or injuries, such as fire, toxic fumes, lack of oxygen, while causing possibly no or minor damage to the aircraft. |
| Uncontrolled collision with ground | Loss of control of the aircraft while in-flight or while the aircraft is on the ground. This includes runway veer-off, runway overrun, and hard landing. Loss of control may be induced by the flight crew, by aircraft malfunctions or by environmental factors such as icing. |
| Forced landing | A landing necessitated by failure of engines, systems, or components which makes continued flight impossible. |
| Controlled flight into terrain | In-flight collision with terrain, water or obstacle without loss of control. |
| Mid-air collision | Collision between aircraft in flight. |
| Collision on ground | Collision on the airport involving the incorrect presence of an aircraft, vehicle, person or animal (excluding birds) on the runway used for landing or intended take-off, or a collision on the airport with an aircraft, person, animal, ground vehicle, building, structure etc. while on a surface other than the runway used for landing or intended take-off. |
| Structure overload | Pre-impact structural failure, with no prior loss of control, collision or explosion, resulting directly in major disintegration of the aircraft, or structural overload resulting in aircraft damage. |
| Fire/Explosion | Pre-impact, on-board fire or explosion that directly results in major disintegration of or damage to the aircraft. |

NB: Security related events will not be included in the analysis because they are considered to be outside the scope of this study.

4.2 Flight phase

Whether or not an event should be regarded as an initiating event of an accident scenario may depend on the context, such as for instance the flight phase, the type of airspace, or local weather conditions. While an aircraft may or may not encounter certain weather conditions, or enter certain types of airspace, each aircraft will always progress through the flight phases taxi, take-off, climb, cruise, descent, approach, and landing. The relevance of the flight phase is underlined by accident statistics that show significant differences in accident frequencies for each phase of flight (Figure 5). Most accidents occur during take-off and landing. However, take-off and landing only account for a small portion of the flight time. The different accident frequencies for the various flight phases justify the use of flight phases as an additional criterion for categorizing accident scenarios. Therefore we propose to use the phase of flight as a second criterion for accident categorization.

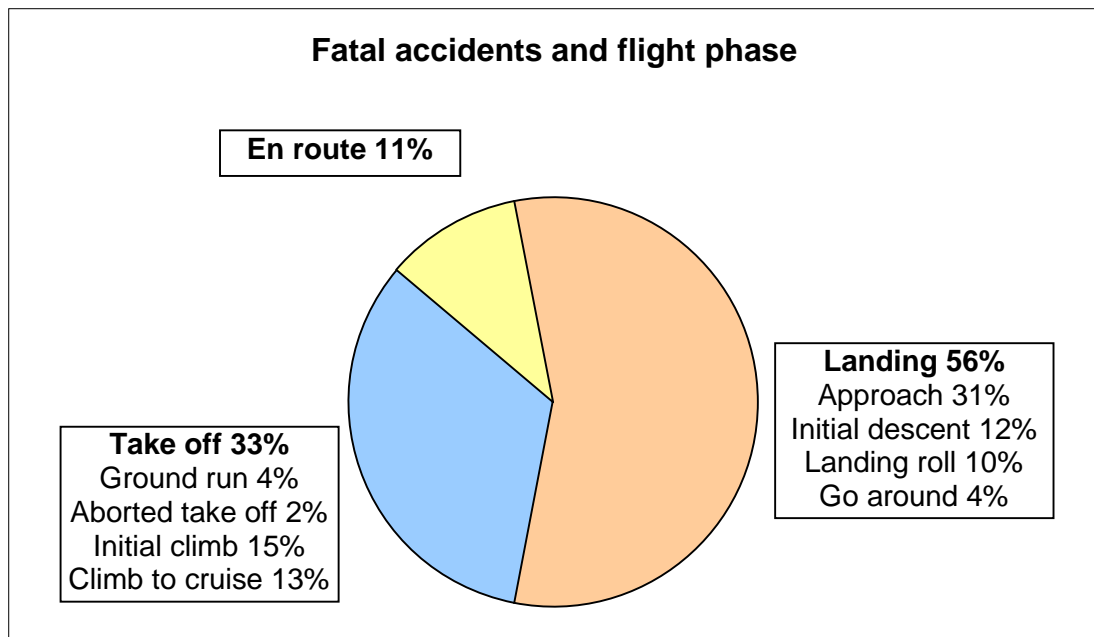


Figure 5 Fatal accidents and flight phase, worldwide 1989-2003 (source IVW 2004).

Phase of flight definitions are taken from the CAST/ICAO Common Taxonomy Team and are listed in Table 2.

Table 2: Flight phase definitions.

| | |
|---------------|--|
| TAXI | The aircraft is moving on the aerodrome surface under its own power prior to take-off or after landing |
| TAKEOFF | From the application of take-off power, through rotation and to an altitude of 35 ft above runway elevation. |
| INITIAL CLIMB | From the end of the take-off phase to the first prescribed power reduction, or until reaching 1000 ft above runway elevation or the VFR pattern, whichever comes first. |
| EN ROUTE | From completion of initial climb through cruise altitude and completion of controlled descent to the Initial Approach Fix (IAF). |
| APPROACH | From the Initial Approach Fix (IAF) to the beginning of the landing flare. |
| LANDING | From the beginning of the landing flare until aircraft exits the landing runway, comes to a stop on the runway, or when power is applied for take-off in case of a touch-and-go landing. |



The combination of accident type and flight phase creates a convenient way for clustering accident scenarios, see Table 3.

Table 3: Proposed scenario matrix.

| | Taxi | Take-off | Initial Climb | En-route | Approach | Landing |
|------------------------------------|------|----------|---------------|----------|----------|---------|
| Abrupt maneuver | | X | X | X | X | |
| Cabin environment (fire, O2) | X | X | X | X | X | X |
| Uncontrolled collision with ground | | X | X | X | X | X |
| Controlled flight into terrain | | | X | X | X | |
| Forced landing | | | | | | X |
| Mid-air collision | | | X | X | X | |
| Collision on ground | X | X | | | | X |
| Structure overload | | X | X | X | X | X |
| Fire/Explosion | X | X | X | X | X | X |

Accident types do not only represent different causal chains leading to the accident, but also show differences in accident severity. An analysis of some 1,000 accidents has shown that the type of accident is typically linked to damage severity classes [Roelen et al. 2001]. The same analysis showed that the number of deaths and serious injuries suffered by the occupants is directly linked to the severity of the damage to the aircraft. Only in a small number of accidents have passengers been killed without the aircraft also being destroyed and in these cases only a small number of people died. The ability to link types of accidents with typical levels of accident severity is a useful characteristic when the model is used for prioritization within a set of possible safety improvement measures.



5 Event Sequence Diagram

As was explained in section 3.5, we propose to use conventional Event Sequence Diagram (ESD) techniques for representing accident scenarios because they provide an easy understanding. The following sections provide general theory and background information on ESDs.

5.1 General theory

An Event Sequence Diagram (Figure 6) is a flowchart with paths leading to different *end states*. Each path through the flowchart is a scenario. Along each path, *pivotal events* are identified as either occurring or not occurring. The event sequence starts with an *initiating event* such as a perturbation that requires some kind of response from operators or pilots or one or more systems [Stamatelatos et al. 2002].

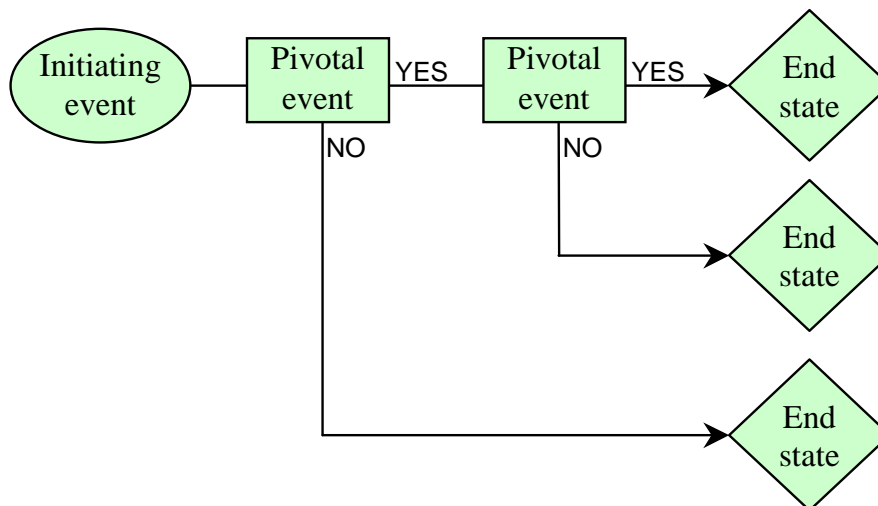


Figure 6 Event Sequence Diagram.

Conditional operators can be included to represent different outcomes depending on whether the condition is met or not. Figures 7 and 8 show types of events and condition in an ESD and their iconic representation

Intentionally, the building blocks of the scenarios are kept broad and generic to cover many ‘similar’ situations. The detailed specific or possible causes or contributing factors of these events are not directly of interest at the scenario level. They are added, when such details are necessary, through other layers of the model, such as Fault Trees or Bayesian Belief Nets. Event Sequence Diagrams are often combined with fault trees. In practice, Event Sequence Diagrams are typically used to portray progression of events over time, while fault trees best represent the



logic corresponding to failure of complex systems [Stamatelatos et al. 2002]. Fault trees are used to model initial and pivotal events in Event Sequence Diagrams in sufficient detail. The initiating and pivotal events in the Event Sequence Diagram are the top events in the fault trees in the proposed hybrid model as shown in Figure 1. Initiating events can be regarded as the center of a bow-tie diagram (Figure 9) that is sometimes used to represent accident sequences (see for instance Roelen et al 2000).

By a clever selection of initiating and pivotal events, the task of developing the underlying layers of the model will be less complicated. In particular it is important to look at possible interdependencies at the first underlying level (i.e. first level below the ESD). Fault tree parts that appear in multiple pivotal events correspond to potentially significant interdependencies. It is therefore sensible to have at least some understanding of the first underlying layer of the model when developing the scenarios.

Only active events are put in the accident sequence. Latent events are dealt with in the Fault Trees and Bayesian Belief Nets. This is done to limit the size of the accident scenarios and to make them easier to understand. Furthermore, latent failures are often ‘common mode’ and/or ‘soft’ causal relations, which can be better expressed in influence diagrams rather than ESDs.

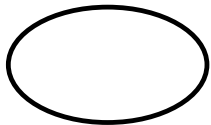
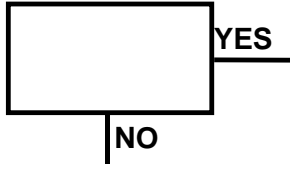
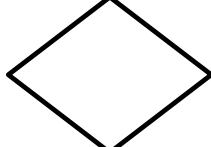
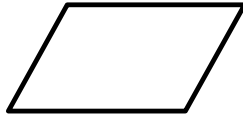
| | |
|---|---|
|  | <p>Initiating event: The first event in an ESD which initiates a sequence of events terminating in an end state</p> |
|  | <p>Pivotal event: An event which has two outcomes, typically ‘yes’ and ‘no’, corresponding to event occurrence and non-occurrence.</p> |
|  | <p>End state: It is the terminating point of an ESD scenario. An ESD can have multiple end states.</p> |
|  | <p>Comment box: Used for providing information regarding the development of the accident sequence.</p> |

Figure 7: Types of events in an ESD and their iconic representation.

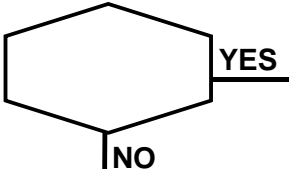
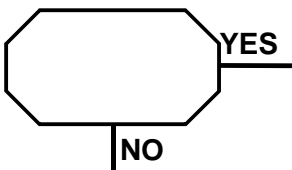
| | |
|---|---|
|  | <p>Time condition: Represents a condition of the form $a < t < b$. Leads to two outcomes depending on whether the condition is met or not.</p> |
|  | <p>Physical variable condition: Represents a condition of the form $a < p < b$. Leads to two outcomes depending on whether the condition is met or not.</p> |

Figure 8: Types of conditions in an ESD and their iconic representation.

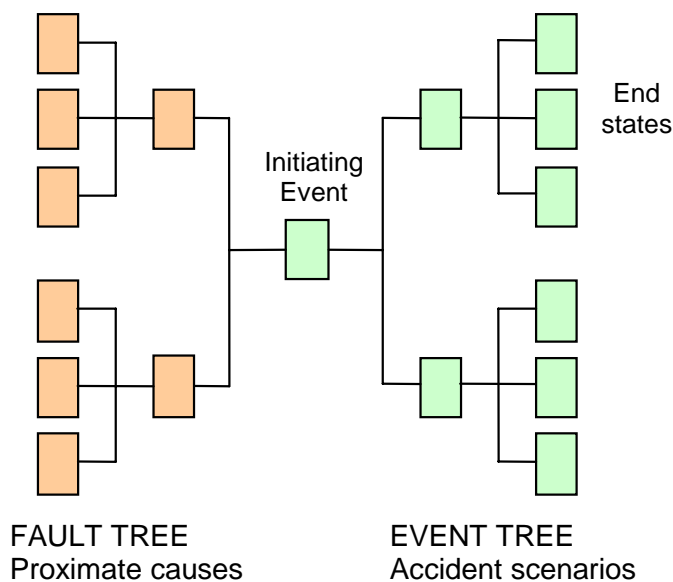


Figure 9: Bow-tie schematic.

5.2 Criteria for selecting initiating events

According to [Stamatelatos 2002], a useful starting point for identification of initiating events is a specification of ‘normal’ operations in terms of the nominal values of a suitably chosen set of physical parameters and the envelope in this variable space outside of which an initiating event would be deemed to have occurred.

A physical parameter that runs out of its normal performance envelope is not sufficient however to define an initiating event. It might as well be a pivotal event. Important is that the initiating event indeed *initiates* a deviation from ‘normal’ operations to a sequence of events that potentially ends with an accident.



It may sometimes be difficult to define, for each relevant parameter, the threshold values for 'normal operation'. An event or condition may be a hazard in one context and under a set of specific conditions, but not in another context. It is the series of events following the initiating event that defines the initiating event.

We are looking at active failures or occurrences rather than latent failures. Latent failures are failures that are created (a long time) before the accident, but lie dormant until an active failure triggers their operation [Reason 1990]. By this definition, latent failures are not represented directly in the event sequence diagram, but in the underlying fault trees and Bayesian Belief Nets. The added advantage is that this approach is more suitable to represent the common cause character of many latent failures.

The list of initiating events must be able to capture events that are possible but have not (knowingly) occurred. Criteria for choosing the initiating events are:

- That it is possible to define a limited number of mutually exclusive events which cover all possibilities at that point.
- They should represent a clear transition from 'normal control' to abnormal conditions.
- After that point the demand on a number of known designed barriers or recovery measures (like trained responses) can be modeled, leading to different event pathways and different outcomes.

Additional selection criteria are that initiating events are:

- Highlighting something that is important to the decision maker.
- Active failure between the moment of engine start to engine shutdown.
- Within the scope of interest and domain of analysis, i.e. 14 CFR Part 121 operators.

5.3 Criteria for selecting pivotal events

Similarly to initiating events, we are only looking for active failures as pivotal events. Pivotal events are those events that could change the outcome. A flight is regarded as operating within a safe envelope, where pivotal events either push the operation outward towards the boundaries or back inside that safe envelope. Thinking in terms of safety barriers can sometimes also be useful for identifying pivotal events.

Pivotal events are not necessarily independent of each other. Indeed, in dynamic situations pivotal events are strongly interdependent. In particular common cause failures may influence multiple pivotal events. These interdependencies must be captured in the underlying levels of the risk model, i.e. in the fault trees and Bayesian Belief Nets. Nevertheless, it is advantageous to define pivotal events in such a way that they are independent. This will avoid cross links



between the fault trees that feed into the ESD. While such cross links may sometimes be unavoidable, they complicate modeling, especially when it comes to quantification, and should therefore be minimized.

For a decision-maker it is important that the pivotal events help to identify where possible controls can be put in place.

All events following the initiating event in the ESD, including the fault trees that tie into the pivotal events, are conditional to the initial event. This is important for the logic structure and especially for quantification.

5.4 End state

The end state of the ESD should be able to capture 'failures', i.e. accidents, as well as 'successes', i.e. cases where an accident is avoided. As the ICAO definition of an accident includes damage to the aircraft and death and injury, the end states that designate 'failures' should capture damage and casualties. In anticipation of the future use of the model, it would be beneficial to capture possible characteristics of those end states that represent 'success' (i.e. the accident is avoided) but cause additional costs to the airline. An example is a diversion to an alternate airport.



6 Scenario development

6.1 ESD development steps

The development of ESDs is a three-step process:

1. Individual accidents and incidents are analyzed and represented as a sequence of events. This step results in detailed accident scenarios specific for the analyzed accidents/incidents.
2. Accident scenarios are generalized per type of accident, initiating event and flight phase. At this stage the diagram is also expanded at meaningful branch points and additional pivotal events, resulting from the prospective analysis, are included.
3. Generalized scenarios are combined into one generic ESD so that this ESD covers a class of accidents.

6.2 Retrospective and prospective analysis

Accident scenarios are initially synthesized by analysis of accident and incident reports, i.e. retrospective analysis. Such an approach requires extensive analysis before obtaining an acceptable exhaustive model for each consequence category. In addition, there is a risk of possible 'blind spots' in the model with respect to hazards that have not yet materialized and potential hazards in future aviation. It is therefore required to combine retrospective analysis with hazard identification techniques.

Two different hazard identification techniques were used during the development of the model:

- 1) Extrapolation of existing accident circumstances in order to determine whether variations in the accident sequence would result in differences with respect to fatalities and damage.
- 2) Systematic analysis in order to find original combinations. Systematic analysis is a bottom-up process from the system towards the unwanted outcome (the accident).

In selecting accidents to be used in the retrospective analysis, the initial focus was on the most recent accidents, i.e. accidents that occurred in the past 10 years. However sometimes older accidents were used as well. When using older accidents, care must be taken to make sure the accident is still representative for today's situation. This is of particular importance for e.g. collision accidents that occurred before the installation of Traffic Alert & Collision Avoidance Systems (TCAS) became mandatory, or CFIT accidents before the introduction of Ground Proximity Warning Systems (GPWS). The final decision whether an older accident was representative of today's situation was left to the analyst.

The accident sample was limited to accidents that have occurred to transport category aircraft in commercial operations for which good quality data was available, typically in the form of a full



accident investigation report. Only 'Western built' aircraft were included. In total the analysis included 73 fatal accidents and 49 non-fatal accidents/incidents, representing 4698 fatalities. The accident sample includes 54% of the fatal accidents (representing 82% of the fatalities) of western operators² between 1994 and 2004.

Because of the combination of retrospective and prospective analysis (see section 6.2) and due to the generic character of the scenarios, most accidents and incidents that are not directly covered in the retrospective analysis can still be matched with one of the scenarios. The full list of accidents and incidents included in the sample is provided in Appendix A.

Initiating and pivotal events of each individual accident were selected according to the criteria provided in sections 5.2 and 5.3. Inevitably, subjective judgments of the analysts also played a role in deciding which events were considered to be initial and pivotal in the accident sequence. In particular the decision on whether or not an event should be explicitly represented as a pivotal event, or should be implicitly represented in the underlying fault tree, was sometimes difficult to make. A guiding consideration was the fact that we did not want the ESDs to become too large, as one of the objectives of the ESDs is to use them for communication between the analysts and the potential users of the model. A second important consideration was that we tried to define the events that are as independent of each other as possible, to facilitate the construction of the underlying fault trees at a later stage.

6.3 Definitions of initiating and pivotal events

The definition of the events of the scenario must be done such that there is no possibility for misunderstanding or misinterpretation. A complicating factor is that to keep the ESDs easy to read, it is undesirable to show complete definitions of events in the Event Sequence Diagram. Instead of complete definitions, keywords are used to label initiating events and pivotal events. The drawback is that when complex events are condensed into keywords, information is inevitable lost. The desire to create event descriptions that fit into the standardized boxes (or whatever shape is used) of the representation scheme promotes the use of compressed phrases such as "flight crew inappropriate response", which may be ambiguous. Such event descriptions may thus be misinterpreted. At this stage, complete and formal definitions of the initiating and pivotal events have not yet been established.

Since a pivotal event is the top-event of the underlying fault tree, it is preferred that the pivotal event is expressed as a failure instead of a success. Fault trees typically represent failure propagation with a failure as top-event. Consequently, following the pivotal events in an event

² Western operators are air carriers from North America, Western-Europe, Australia and New Zealand.



sequence diagram to the right represents the continuation of ‘failures’ towards an accident, whereas an outcome of a pivotal event downwards (‘no failure’) represent an intervention in the sequence to an accident, leading to another sequence to potential safe outcomes.

The phraseology that is used in the ESDs, in particular the use of the words ‘unable to’, is not intended to blame or to indicate failed responsibilities, nor does it exclude the possibility of human error. The words ‘unable to’ are sometimes necessary to avoid using a double negation, i.e. to avoid application of two NOT operators to a statement. The word ‘not’, which, in combination with ‘yes’ and ‘no’ branches as possible outcomes can be confusing. Figure 10 further illustrates this issue.

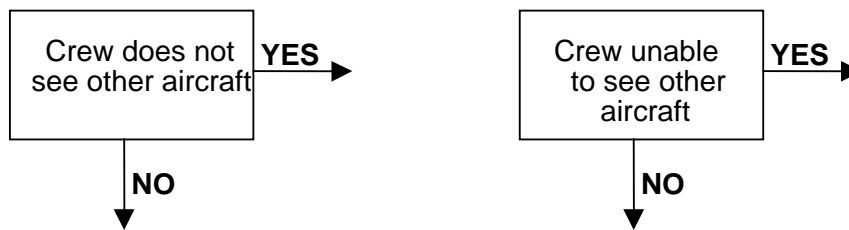


Figure 10: Example of the use of the word ‘unable’ to avoid possible confusion due to the double negation.

Secondly, the words ‘crew fails to’ do not necessarily mean that the failure is the responsibility of the crew. As an example, ‘crew fails to maintain control’ can indicate a flight crew error as well as a technical malfunction that renders the aircraft uncontrollable.

6.4 Existing definitions and taxonomies

The initiating events, pivotal events and end states are the ‘building blocks’ of the Event Sequence Diagram. Different scenarios may share common events, although the scenarios themselves could be mutually exclusive. Components that are used to describe a particular scenario should be defined such that they can be used in other scenarios as well. The underlying model structure (fault tree) caters for any possible differences. By careful consideration of the ‘building blocks’ of the scenarios, the overall complexity of the causal risk model can be minimized. The required level of detail or abstraction is also an important issue that needs careful consideration. Intentionally we keep the building blocks of the scenarios broad and generic to cover many ‘similar’ situations, historically observed or deemed possible by experts.

Systematic categorization of the events facilitates the development of a list of events that is sufficiently complete. In addition, by proper selection of different categories, interdependencies



between different events can to a certain extent be avoided, and this will be a big advantage once the individual events are further developed into fault trees.

In establishing definitions for initiating and pivotal events, it is advantageous to recognize existing definitions or descriptions. Model acceptance by the industry will be improved if existing definitions and/or taxonomies are used. An additional advantage of using existing taxonomies is the possibility to relate to current databases for quantification. Taxonomies that are widely used are ICAO's ADREP, EUROCONTROL's HEIDI, the NTSB taxonomy and the taxonomy of 'problem statements' developed by CAST. These are described in Appendix C.

While at this stage complete definitions of all initiating and pivotal events have not yet been developed, it is recommended that this should be one of the priorities of the next stage of development. The definitions should preferably correspond as much as possible with existing taxonomies.

6.5 Results

36 Event Sequence Diagrams with 28 different initiating events have been developed. A list of all ESDs is presented in table 4. Full diagrams of the scenarios are provided in Appendix B.



Table 4: Overview of accident scenarios.

| ESD | Accident type | Flight phase | Initiating event |
|-----|------------------------------------|--|---|
| 1 | Uncontrolled collision with ground | Take-off | Aircraft system failure |
| 2 | Uncontrolled collision with ground | Take-off | ATC event |
| 3 | Uncontrolled collision with ground | Take-off | Aircraft handling by flight crew inappropriate |
| 4 | Uncontrolled collision with ground | Take-off | Aircraft directional control related system failure |
| 5 | Uncontrolled collision with ground | Take-off | Operation of aircraft systems by flight crew inappropriate |
| 6 | Uncontrolled collision with ground | Take-off | Aircraft takes off with contaminated wing |
| 7 | Uncontrolled collision with ground | Take-off | Aircraft weight and balance outside limits |
| 8 | Uncontrolled collision with ground | Take-off | Aircraft encounters performance decreasing windshear after rotation |
| 9 | Uncontrolled collision with ground | Take-off | Single engine failure |
| 10 | Uncontrolled collision with ground | Take-off | Pitch control problem |
| 11 | Fire/explosion | Take-off/initial climb/en-route/approach/landing | Fire on board aircraft |
| 12 | Uncontrolled collision with ground | Initial climb/en-route/approach/landing | Flight crew member spatially disoriented |
| 13 | Uncontrolled collision with ground | Initial climb/en-route/approach/landing | Flight control system failure |
| 14 | Uncontrolled collision with ground | Take-off/initial climb/en-route/approach/landing | Flight crew incapacitation |
| 15 | Uncontrolled collision with ground | Initial climb/en-route/approach | Anti-ice/de-ice system not operating |
| 16 | Uncontrolled collision with ground | Initial climb/en-route/approach/landing | Flight instrument failure |
| 17 | Structure overload | Initial climb/en-route/approach | Aircraft encounters adverse weather |
| 18 | Uncontrolled collision with ground | Initial climb/en-route/approach | Single engine failure |
| 19 | Uncontrolled collision with ground | Approach | Unstable approach |
| 20 | Uncontrolled collision with ground | Approach | Flight crew fails to execute missed approach according to Standard Operating Procedures |
| 21 | Uncontrolled collision with ground | Approach | Aircraft weight and balance outside limits |
| 22 | Uncontrolled collision with ground | Approach | Flight control system failure |
| 23 | Uncontrolled collision with ground | Landing | Aircraft encounters windshear during approach/landing |
| 24 | Uncontrolled collision with ground | Landing | Unstable approach |
| 25 | Uncontrolled collision with ground | Landing | Aircraft handling by flight crew during flare inappropriate |
| 26 | Uncontrolled collision with ground | Landing | Aircraft handling by flight crew during landing roll inappropriate |
| 27 | Uncontrolled collision with ground | Landing | Aircraft directional control related system failure |
| 28 | Uncontrolled collision with ground | Landing | Single engine failure |
| 29 | Uncontrolled collision with ground | Landing | Thrust reverser failure |
| 30 | Uncontrolled collision with ground | Landing | Aircraft encounters unexpected wind |
| 31 | Mid-air collision | Initial climb/en-route/approach | Aircraft are positioned on collision course |
| 32 | Collision on ground | Taxi /take-off/landing | Incorrect presence of aircraft/vehicle on runway in use |

| ESD | Accident type | Flight phase | Initiating event |
|-----|--------------------|--|---|
| 33 | Structure overload | Initial climb/en-route/approach | Cracks in aircraft pressure cabin |
| 34 | Structure overload | Take-off/initial climb/en-route/approach/landing | Aircraft encounters unexpected wind |
| 35 | CFIT | Initial climb/en-route/approach | Flight crew decision error/operation of equipment error |
| 36 | Personal injury | Initial climb/en-route/approach | Aircraft encounters turbulence |

6.6 Example of hybrid logic

In order to demonstrate the hybrid concept of the integrated risk model, one of the ESDs has been integrated with a Fault Tree. The 'loss of control' scenario with initiating event 'single engine failure' in flight phases initial climb, en route and approach (representing twin engine aircraft) was integrated with a fault tree for engine failure which was developed in [Roelen, 2004a]. The result is presented in Figure 11. In the future, Fault Trees and/or Bayesian Belief Nets need to be developed for other initiating and pivotal events and integrated with the ESDs in a similar way.

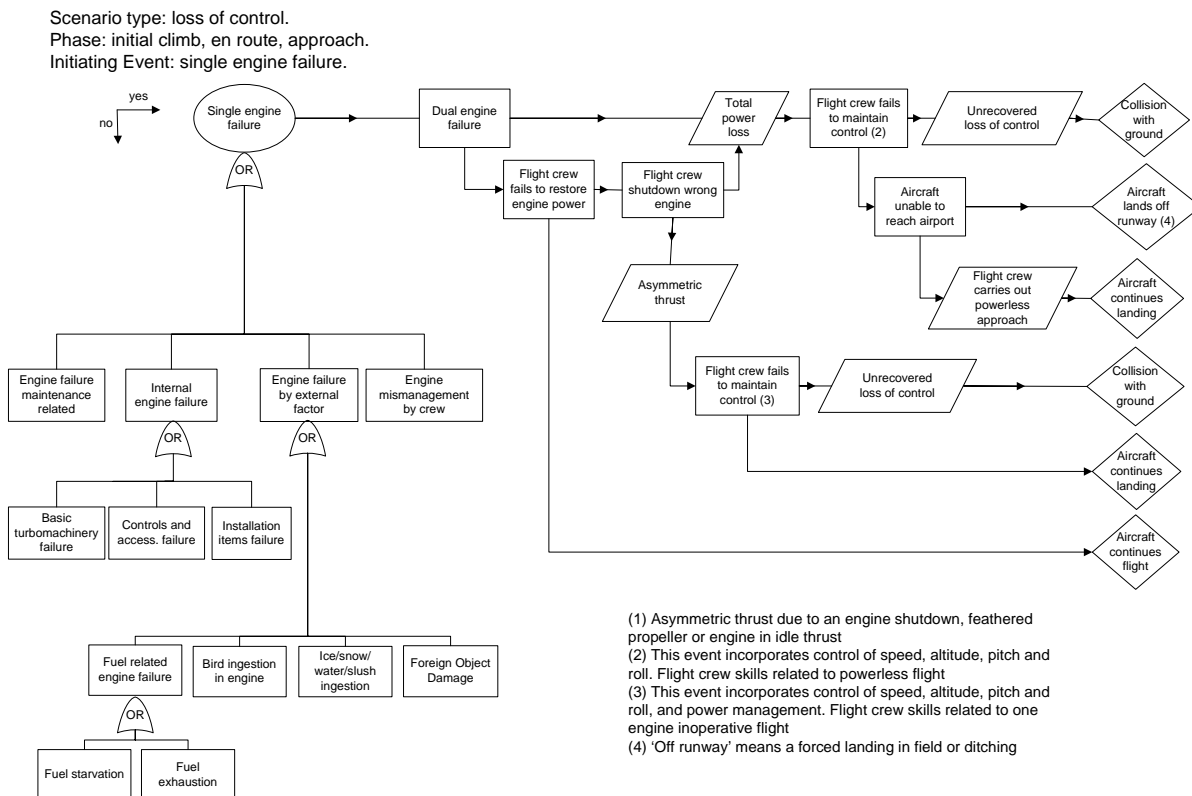


Figure 11: Example of integration of Fault Tree and Event Sequence Diagram.



7 Discussion

Design requirements for the scenarios include that they should serve as top-layer of the integrated safety model and can be used for communication. Scenarios highlight the most important events in the accident sequence of events, whereas the underlying layers in the model specify the causal pathways leading up to the events in the scenarios. As a result, the scenarios are simplistic. The number of events is limited and the sequence between initiating event and end states covers only a few pivotal events.

Scenarios are on purpose generic to meet the design requirements. When scenarios are described in more detail, the generic character is lost. The desire to define pivotal events such that they do not share common mode elements also contributes to the simplicity of the model.

These scenarios are not intended for isolated use, but will be part of a more complex hybrid logic model. The set of scenarios at the top level of the hybrid logic model should not be too large in order to keep transparency.

Many scenarios contain an initial event followed by a pivotal event related to a crew action or crew intervention, followed by the outcome, i.e. accident or safe flight. This is accordance with Reason's model (Figure 2) and the decision to represent active failures in the scenarios.

Event Sequence Diagrams have not yet been quantified, they are qualitative only. To enable the use of the ESDs for accident risk assessment they should be quantified, i.e. conditional probabilities for each of the events and end-states must be established. This should be done by using existing accident and incident data.



8 Conclusions and recommendations

8.1 Conclusions

- The Event Sequence Diagram methodology is an appropriate technique for modeling accidents scenarios. Criteria have been established for the selection of initiating and pivotal events.
- Main types of accidents have been defined for the integrated safety model, based on the ICAO definition of an accident: abrupt maneuver, cabin environment, uncontrolled collision with ground, forced landing, controlled flight into terrain, mid-air collision, collision on ground, structure overload, and fire/explosion. Accident scenarios are grouped by accident type and different flight phases.
- 36 different accident scenarios have been modeled through a combination of retrospective and prospective analysis. These scenarios are the top layer of the proposed integrated safety model.
- Retrospective analysis included a review of 73 fatal accidents and 49 non-fatal accidents and incidents, representing 4698 fatalities. The accident sample includes 54% of the fatal accidents (representing 82% of the fatalities) of western operators between 1994 and 2004.
- The scenarios are generic. A high level of abstraction is required to make the scenarios easy to understand for users and to keep the model transparent and simple. Complexity and details will be added in underlying submodels.

8.2 Recommendations

- Quantification of the ESDs is necessary to enable the use of the ESDs in accident risk assessment. This should be a next step in the development of the integrated safety model.
- It is recommended to develop the first layer(s) of the fault trees underlying the initiating and pivotal events in the scenarios. This is an essential step in order to expand the integrated safety model. The first layer of the fault trees will further clarify and define the causal pathways to the initiating and pivotal events in the scenarios. In the development of these fault trees a combination of retrospective and prospective analysis should be used.
- Proper definitions for the initiating and pivotal events should be developed. It is recommended that this is one of the priorities of the next stage of development. The definitions should preferably correspond as much as possible with existing taxonomies.
- A set of end states should be developed, which refer to the severity of the outcome of a scenario in terms of fatalities, injuries and aircraft damage, as well other outcomes that may be of interest to model users, such as delay, diversion etc. The objective should be to obtain a limited and agreed set of end states based on a systematic approach that can be used in the integrated safety model.



9 References

Ale, B.J.M. 2004. Development of a causal model for air transport safety, Research proposal for Ministry of Transport and Water, Delft University of Technology, the Netherlands.

Civil Aviation Authority. 1998. Global Fatal Accident Review, 1980-96, CAP 681, CAA, London.

Civil Aviation Authority. 2000. Aviation Safety Review, 1990-1999, CAP 701, CAA, London.

Civil Aviation Authority. 2002. Safety Management Systems for Commercial Air Transport Operations, CAP 712, CAA, London.

De Jong, H.H. 2004. Guidelines for the identification of hazards; How to make unimaginable hazards imaginable? NLR Contract Report for EUROCONTROL, NLR-CR-2004-094.

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

Dutch project group causal modelling. 2003. 'Inhoudelijke rapportage Projectgroep'. (in Dutch).

EUROCONTROL, Explanatory Material on ESARR 4 Requirements, Edition 1.0, 18 February 2003, EUROCONTROL Safety Regulation Commission.

Fragola, J.R. Space Shuttle Probabilistic Risk Assessment.

ICAO. 1987. Accident/Incident Reporting Manual (ADREP Manual), second edition, Doc 9156-AN/900. International Civil Aviation Organization, Montreal. Canada.

ICAO/CAST Common Taxonomy Team, phase of flight definitions and usage notes, 2002.

ICAO/CAST Common Taxonomy Team, Aviation occurrence categories, definitions and usage notes, 2004.

Kemeny, J. 1979. Report of the President's Commission on the accident at Three Mile Island, Washington D.C.



Labeau, P.E., Smidts, C., Swaminathan, S. 2000. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety*, 68, pp 219-254.

Leveson, N, 2004. A new accident model for engineering safer systems, *Safety Science*, Vol. 42, No 4., pp 237-270.

Lewis, H.W., Budnitz, R.J., Kouts, H.J., Lowenstein, W.B., Rowe, W.D., Von Hippel, F., Zachariassen, F. 1979. Risk assessment review group report to the U.S. Nuclear Regulatory Commission, NUREG/CR-0400.

Lloyd, E. Tye, W. 1982. *Systematic Safety*, Civil Aviation Authority, London.

Mosleh, A, Dias, A, Eghbali, G, Fazen, K. 2004. An integrated framework for identification, classification, and assessment of aviation system hazards, Probabilistic safety assessment and management: PSAM 7 - ESREL '04: proceedings of the 7th International Conference on Probabilistic Safety Assessment and Management, 14-18 June 2004, Berlin, Germany.

NRC. 1975. Reactor Safety Study, U.S. Nuclear Regulatory Commission, WASH-1400, NUREG –751014.

NRC. 1983. PRA Procedures guide, a guide to the performance of probabilistic risk assessments for nuclear power plants, Final Report, Vol. 1-2, NUREG/CR-2300.

NRC. 1995. Use of probabilistic risk assessment methods in nuclear regulatory activities, final policy statement, Federal Register, Vol. 60, No. 158.

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

Reason, J. 1997. Maintenance related errors: The biggest threat to aviation safety after gravity?, In 'Aviation Safety', H. Soekha (ed.), VSP, Utrecht, The Netherlands.

Roelen, A.L.C. Bellamy, L.J., Hale, A.R., Molemaker, R.J., Van Paassen, M.M. 2000. Feasibility of the development of a causal model for the assessment of third party risk around airports, Part 1: Main report, NLR-CR-2000-189-PT-1, NLR Amsterdam.

Roelen, A.L.C., Piers, R., Molemaker, R.J., Hayes, P. 2001. Handbook for conducting cost benefit analysis of safety measures in air transport, NLR-CR-2001-609, NLR Amsterdam.



Roelen, A.L.C., Wever, Hale, A.R., Goossens, L.H.J., Cooke, R.M., Lopuhaa, R., Simons, M., Valk, P.J.L. 2002. Causal modeling of air safety, Demonstration model, NLR-CR-2002-662, NLR Amsterdam.

Roelen, A.L.C., Wever, R. 2004a. A causal model of engine failure, NLR-CR-2004-038, NLR Amsterdam.

Roelen, A.L.C., Wever, R. 2004b. A causal model of a rejected take-off, NLR-CR-2004-039, NLR Amsterdam.

Rogers, W.P. 1986. Report of the Presidential Commission on the Space Shuttle Challenger Accident, Washington D.C.

Stamatelatos, M. et. al , 2002. Probabilistic risk assessment procedures guide for NASA managers and practitioners, Version 1.1.

Transport and Water Inspectorate the Netherlands. 2004. Civil Aviation Safety Data 1989-2003, Civil Aviation Authority the Netherlands, Hoofddorp.

Van der Geest, P.J., Piers, M.A., de Jong, H.H., Finger, M., Slater, D.H., Van Es, G.W.H., Van der Nat, G.J. 2003. Aviation safety management in Switzerland; Recovering from the myth of perfection. NLR-CR-2003-316. NLR Amsterdam.



Appendix A List of accidents used for the development of ESDs

Loss of control take-off

- Boeing 737-222, Air Florida, Washington, DC, 13 January 1982.
- Boeing 727, Delta Airlines, Dallas/Fort Worth Int. Airport, Texas, 31 August 1988.
- Boeing 737-400, USAir, LaGuardia, New York, 20 September 1989.
- Douglas DC-8-62, Air Transport International, JFK Int. Airport, New York, 12 March 1991.
- Fokker F-28, USAIR, LaGuardia Airport, New York, 22 March 1992.
- Fokker 100, Palair, Skopje, Rep. of Macedonia, 5 March 1993.
- McDonnell Douglas MD-82, Continental Airlines, LaGuardia Airport, New York, 2 March 1994.
- Douglas DC-8-63, Air Transport International, Kansas City, 16 February 1995.
- McDonnell-Douglas DC-10-30ER, Canadian Airlines, Vancouver Int. Airport, British Columbia, 19 October 1995.
- Boeing 747-100, Tower Air, JFK Int. Airport, New York, 20 December 1995.
- Boeing 737-200, Southwest Airlines, Nashville, Tennessee, 8 July 1996.
- Douglas DC-8-61, Fine Air, Miami, Florida, 7 August 1997.
- Beech 1900D Ministic Air, Island Lake, Manitoba, Canada, 29 November 1997
- British Aerospace Jetstream 31, Stansted, United Kingdom, 30 June 1998.
- Boeing 737-200, LAPA, Buenos Aires, Argentina, 31 August 1999.
- Douglas DC-9, Air Canada, Edmonton Int. Airport, Alberta, Canada, 11 May 2000.
- Raytheon 1900D, Air Midwest, Charlotte, North Carolina, USA, 8 January 2003.
- McDonnell-Douglas DC-9, AeroCalifornia, Mexico City, Mexico, 21 July 2004.

Loss of control en-route

- Douglas DC-8-63, Air Transport International, Swanton, Ohio, 15 February 1992.
- ATR-72, Simmons Airlines, Roselawn, Indiana, 31 October 1994.
- Douglas DC-9-32, Valujet Airlines, Near Miami, Florida, 11 May 1996.
- Douglas DC-10-10, Federal Express, Newburgh, New York, 5 September 1996.
- Embraer EMB-120RT, Comair Airlines, near Monroe, Michigan, 9 January 1997.
- Dassault Falcon 900B, Olympic Airways, Bucharest. Rumania, 14 September 1999.
- Learjet 35, Sunjet Aviation, Aberdeen, South Dakota, 25 October 1999.
- Boeing 747-200, Korean Airlines, Stansted, London, UK, 22 December 1999.
- McDonnell Douglas MD-83, Alaska Airlines, about 2.7 Miles North of Anacapa Island, California, 31 January 2000.
- Raytheon Super King Air 200, Jet Express Services, Strasburg, Colorado, 27 January 2001.
- Airbus Industrie A300-605R, American Airlines, Belle Harbor, New York, 12 November 2001.



Loss of control approach

- British Aerospace Jetstream 41, Atlantic Coast Airlines, Columbus, Ohio, 7 January 1994.
- Saab 340, KLM Cityhopper, Amsterdam, the Netherlands, 4 April 1994.
- Airbus Industrie A300, China Airlines, Nagoya Airport, Japan, 26 April 1994.
- British Aerospace Jetstream 31, Flagship Airlines, Morrisville, North Carolina, 13 December 1994.
- McDonnell-Douglas MD-83, American Airlines, East Granby, Connecticut, 12 November 1995.
- McDonnell-Douglas MD-88, Delta Airlines, La Guardia, New York, 19 October 1996.
- Beech 1900C, Ameriflight, Seattle, Washington, 13 August 1997.
- Boeing 727-223, American Airlines, Chicago, Illinois, 9 February 1998.
- Fokker F-27, Channel Express, Guernsey, UK, 12 January 1999.
- Boeing 757-200, Britannia Airways, Girona, Spain, 14 September 1999.
- Boeing 737-200, Alliance Air, Patna, India, 17 July 2000.
- Airbus Industrie A320, Gulf Air, Bahrain, 23 August 2000.
- Raytheon King Air A100, Aviation Charter inc, Eveleth, Minnesota, 25 October 2002.
- Boeing 727-232, FedEx, Tallahassee, Florida, USA, 26 July 2002.
- Fokker 50, Luxair, Luxemburg, 6 November 2002.

Loss of control landing

- McDonnell-Douglas DC-10, Martinair, Faro, Portugal, 21 December 1992.
- Airbus Industrie A320, Lufthansa, Warsaw, Poland, 14 September 1993
- Swearingen SA227, Bearskin Lake Air Service Ltd, North Bay Airport, Ontario, Canada, 23 February 1994
- McDonnell-Douglas, DC-9-31, USAir, Charlotte, North Carolina, 2 July 1994.
- McDonnell-Douglas MD-88, Delta Airlines, Denver, Colorado, 4 February 1996.
- McDonnell-Douglas MD-11, Fed Ex, Anchorage, Alaska, 16 May 1996.
- DeHavilland DHC-8, National Jet Systems, Broome, Australia, 17 May 1996.
- McDonnell-Douglas DC-9-82, American Airlines, Albuquerque, New Mexico, 5 June 1996.
- Swearingen SA226, Propair, Puvirnituk, Quebec, Canada, 23 October 1996
- Boeing 747-200, American International Airways, Manuas, Brazil, 22 March 1997.
- Boeing 767, Alitalia, Newark, New Jersey, 22 May 1997.
- Mc-Donnell-Douglas MD-11, FedEx, Newark, New Jersey, 31 July 1997.
- McDonnell-Douglas MD-82, Alitalia, Catania-Fontanarossa Airport, Italy, 28 January 1999.
- McDonnell-Douglas MD-82, American Airlines, Little Rock, Arkansas, 1 June 1999
- McDonnell-Douglas DC-9-31, TWA, Nashville, Tennessee, 9 September 1999.
- Boeing 747-400, Qantas, Bangkok, Thailand, 23 September 1999.
- Boeing 737-300, Southwest Airlines, Burbank, California, 5 March 2000



- Douglas DC-9, Hawaiian Airlines, Lihue, Hawaii, 14 June 2000.
- Airbus Industrie A340, China Airlines, Sydney, Australia, 1 November 2000.
- Airbus Industrie A320, Iberia, Bilbao, Spain, 7 February 2001.
- Embraer EMB145, Mesa Airlines, Roanoke, Virginia, 16 October 2001.
- Swearingen SA-226, Perimeter Airlines, Winnipeg, Canada, 16 April 2002
- British Aerospace Jetstream 41, United Express, Charlottesville, Virginia, 26 August 2002.
- Boeing 737-300, Southwest Airlines, Phoenix, Arizona, 25 November 2003.
- Embraer 145LR, ExpressJet Airlines, Cleveland Ohio, 2 June 2004

Mid air collision

- Douglas DC-9, Aeromexico and Piper PA-28, California, 31 August 1986.
- Swearingen Metro II, Skywest and Mooney M20, Kearns, Utah, 15 January 1987.
- Boeing 757-200, DHL and Tupolev Tu-154M, Bashkirian Airlines, near Uberlingen, Germany, 1 July 2002.
- Tupolev Tu-154M, German Luftwaffe, and Lockheed C-141, USAF, 62 NM west of Namibia, 13 September 1997

Runway collision

- Boeing 747-200, KLM and Boeing 747-100, PanAm, Tenerife, Spain, 27 March 1977.
- McDonnell-Douglas DC-10, Korean Air Lines and Piper PA-31, Southcentral Air, Anchorage, Alaska, USA, 23 December 1983.
- Boeing 727 Northwest and McDonnell-Douglas DC-9, Northwest, Romulus, Michigan, USA, 3 December 1990.
- Boeing 737, USAIR and Fairchild Metroliner, Skywest, Los Angeles, USA, 1 February 1991.
- McDonnell-Douglas MD-82, TWA and Cessna 441, Missouri, USA, 22 November 1994.
- Beechcraft 1900C, United Express and Beechcraft King Air, Quincy, Illinois, USA, 19 November 1996.
- McDonnell-Douglas MD-83, Air Liberte and Shorts 330, Streamline Aviation, Paris, France, 25 May 2000.
- McDonnell-Douglas MD-87, SAS and Cessna 525, Milan Linate Airport, Italy, 8 October 2001.
- Boeing 747-400, Singapore Airlines, Taoyuan, Taiwan, 31 October 2000.

Disintegration

- Fokker F-28, NLM, Moerdijk, the Netherlands, 6 October 1981.
- Boeing 737-200, Aloha Airlines, near Maui, Hawaii, 28 April 1988.
- Boeing 747-100, United Airlines, Honolulu, Hawaii, 24 February 1989.



- Boeing 747-100, TWA, near New York, 17 July 1996.
- McDonnell Douglas MD-90-30, UNI Air, Hua-Lien, Taiwan, 24 August 2000.
- Boeing 747-200, China Airlines, Taiwan Strait, 25 May 2002.

CFIT approach

- Boeing 737-200, Markair, Unalakleet, Alaska, 2 June 1990.
- Airbus A-320, Air Inter, Strasbourg, France, 20 January 1992.
- Airbus A310, Thai Airways, Kathmandu, Nepal, 31 July 1992.
- De Havilland DHC-8, Ansett, Palmerston North, New Zealand, 9 June 1995.
- Boeing 757, American Airlines, Cali, Colombia, 21 December 1995.
- Boeing 747, Korean Airlines, Guam, 6 August 1997.
- ATR 42, Si Fly, Pristina, Kosovo, 12 November 1999.
- AVRO 146-RJ100, Crossair, Zurich, Switzerland, 24 November 2001.
- Canadair CL-600, Brit Air, Brest, France, 22 June 2003.

CFIT en-route

- Douglas DC-10, Air New Zealand, Ross Island, Antarctica, 28 November 1979.
- Boeing 727-200, Lufthansa Cargo India, Kathmandu, Nepal, 7 July 1999.

Appendix B Event sequence diagrams

Event Sequence Diagrams (ESD) are numbered in accordance with table B.1. The total number of event sequence diagrams is 36, with 28 initiating events (table B.2).

Table B.1: Overview of accident scenarios.

| ESD | Accident type | Flight phase | Initiating event |
|-----|------------------------------------|--|---|
| 1 | Uncontrolled collision with ground | Take-off | Aircraft system failure |
| 2 | Uncontrolled collision with ground | Take-off | ATC event |
| 3 | Uncontrolled collision with ground | Take-off | Aircraft handling by flight crew inappropriate |
| 4 | Uncontrolled collision with ground | Take-off | Aircraft directional control related system failure |
| 5 | Uncontrolled collision with ground | Take-off | Operation of aircraft systems by flight crew inappropriate |
| 6 | Uncontrolled collision with ground | Take-off | Aircraft takes off with contaminated wing |
| 7 | Uncontrolled collision with ground | Take-off | Aircraft weight and balance outside limits |
| 8 | Uncontrolled collision with ground | Take-off | Aircraft encounters performance decreasing windshear after rotation |
| 9 | Uncontrolled collision with ground | Take-off | Single engine failure |
| 10 | Uncontrolled collision with ground | Take-off | Pitch control problem |
| 11 | Fire/explosion | Take-off/initial climb/en-route/approach/landing | Fire on board aircraft |
| 12 | Uncontrolled collision with ground | Initial climb/en-route/approach/landing | Flight crew member spatially disoriented |
| 13 | Uncontrolled collision with ground | Initial climb/en-route/approach/landing | Flight control system failure |
| 14 | Uncontrolled collision with ground | Take-off/initial climb/en-route/approach/landing | Flight crew incapacitation |
| 15 | Uncontrolled collision with ground | Initial climb/en-route/approach | Anti-ice/de-ice system not operating |
| 16 | Uncontrolled collision with ground | Initial climb/en-route/approach/landing | Flight instrument failure |
| 17 | Structure overload | Initial climb/en-route/approach | Aircraft encounters adverse weather |
| 18 | Uncontrolled collision with ground | Initial climb/en-route/approach | Single engine failure |
| 19 | Uncontrolled collision with ground | Approach | Unstable approach |
| 20 | Uncontrolled collision with ground | Approach | Flight crew fails to execute missed approach according to Standard Operating Procedures |
| 21 | Uncontrolled collision with ground | Approach | Aircraft weight and balance outside limits |
| 22 | Uncontrolled collision with ground | Approach | Flight control system failure |
| 23 | Uncontrolled collision with ground | Landing | Aircraft encounters windshear during approach/landing |
| 24 | Uncontrolled collision with ground | Landing | Unstable approach |
| 25 | Uncontrolled collision with ground | Landing | Aircraft handling by flight crew during flare inappropriate |
| 26 | Uncontrolled collision with ground | Landing | Aircraft handling by flight crew during landing roll inappropriate |
| 27 | Uncontrolled collision with ground | Landing | Aircraft directional control related system failure |



| ESD | Accident type | Flight phase | Initiating event |
|-----|------------------------------------|--|---|
| 28 | Uncontrolled collision with ground | Landing | Single engine failure |
| 29 | Uncontrolled collision with ground | Landing | Thrust reverser failure |
| 30 | Uncontrolled collision with ground | Landing | Aircraft encounters unexpected wind |
| 31 | Mid-air collision | Initial climb/en-route/approach | Aircraft are positioned on collision course |
| 32 | Collision on ground | Taxi /take-off/landing | Incorrect presence of aircraft/vehicle on runway in use |
| 33 | Structure overload | Initial climb/en-route/approach | Cracks in aircraft pressure cabin |
| 34 | Structure overload | Take-off/initial climb/en-route/approach/landing | Aircraft encounters unexpected wind |
| 35 | CFIT | Initial climb/en-route/approach | Flight crew decision error/operation of equipment error |
| 36 | Personal injury | Initial climb/en-route/approach | Aircraft encounters turbulence |

Table B.2: Initiating events.

| Initiating event |
|---|
| Aircraft are positioned on collision course |
| Aircraft directional control related system failure |
| Aircraft encounters adverse weather |
| Aircraft encounters performance decreasing windshear after rotation |
| Aircraft encounters turbulence |
| Aircraft encounters unexpected wind |
| Aircraft encounters windshear during approach/landing |
| Aircraft handling by flight crew during flare inappropriate |
| Aircraft handling by flight crew during landing roll inappropriate |
| Aircraft handling by flight crew inappropriate |
| Aircraft system failure |
| Aircraft takes off with contaminated wing |
| Aircraft weight and balance outside limits |
| Anti-ice/de-ice system not operating |
| ATC event |
| Cracks in aircraft pressure cabin |
| Fire on board aircraft |
| Flight control system failure |
| Flight crew decision error/operation of equipment error |
| Flight crew fails to execute missed approach according to SOP |
| Flight crew incapacitation |
| Flight crew member spatially disoriented |
| Flight instrument failure |
| Incorrect presence of aircraft/vehicle on runway in use |
| Operation of aircraft systems by flight crew inappropriate |
| Pitch control problem |
| Single engine failure |
| Thrust reverser failure |

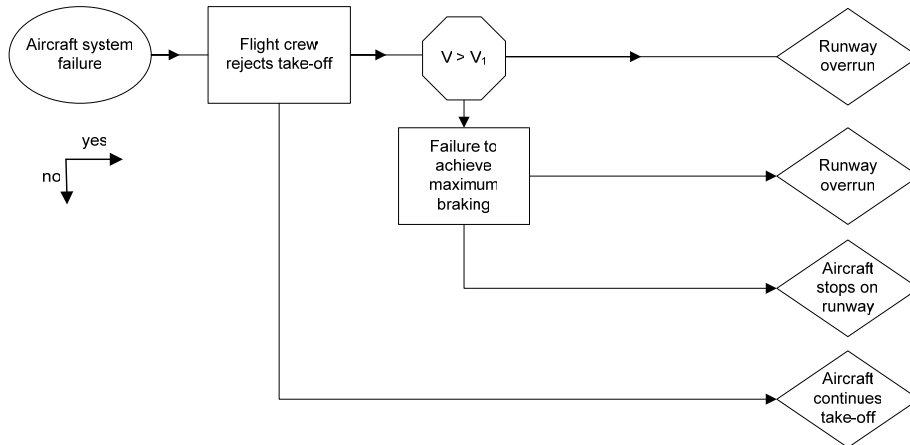


B.1 ESD 1

Accident type: uncontrolled collision with ground.

Flight phase: take-off.

Initiating event: aircraft system failure.

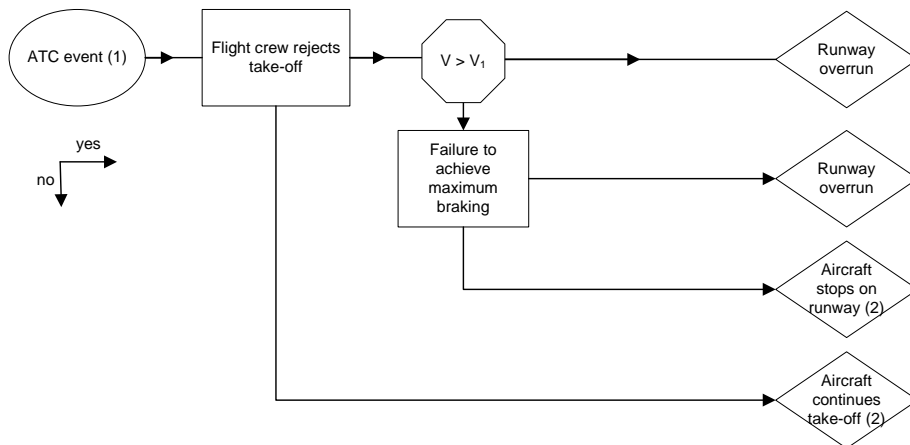


B.2 ESD 2

Accident type: uncontrolled collision with ground.

Flight phase: take-off.

Initiating event: ATC event.



- (1) ATC event includes for instance a runway incursion or air traffic controller's instruction to abort take-off
- (2) potential for runway collision

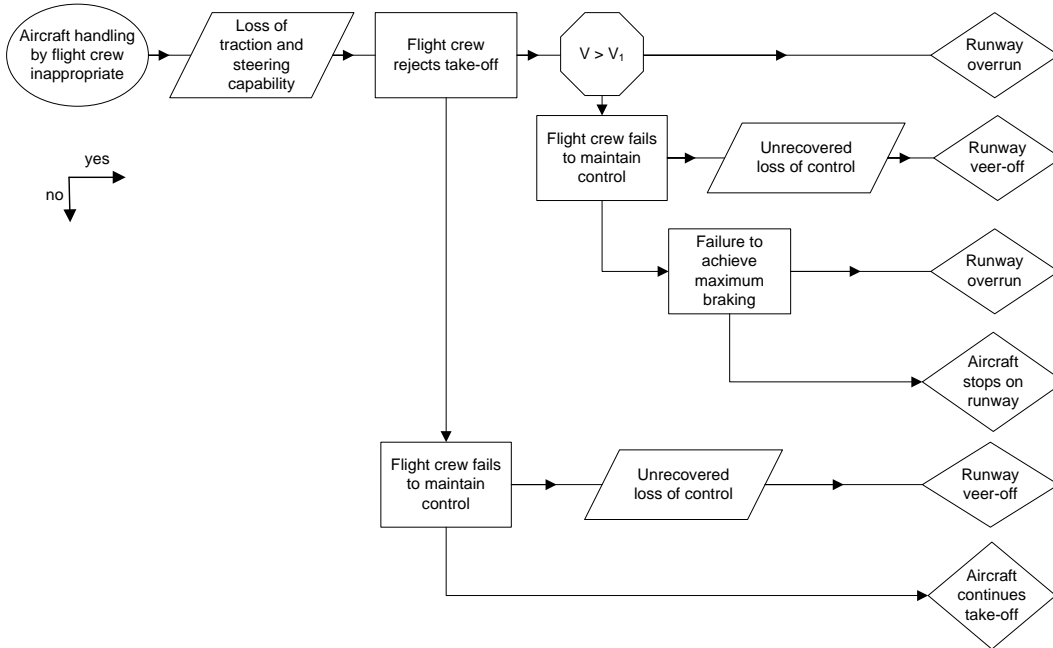


B.3 ESD 3

Accident type: uncontrolled collision with ground.

Flight phase: take-off.

Initiating event: Aircraft handling by flight crew inappropriate.

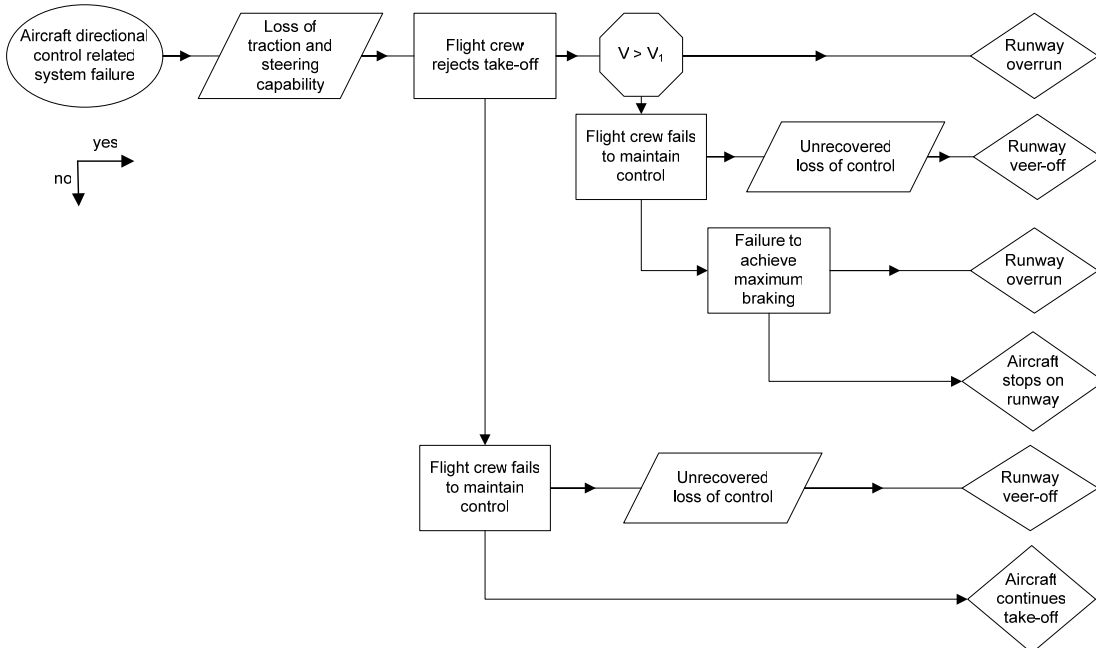


B.4 ESD 4

Accident type: uncontrolled collision with ground.

Flight phase: take-off.

Initiating event: aircraft directional control related system failure

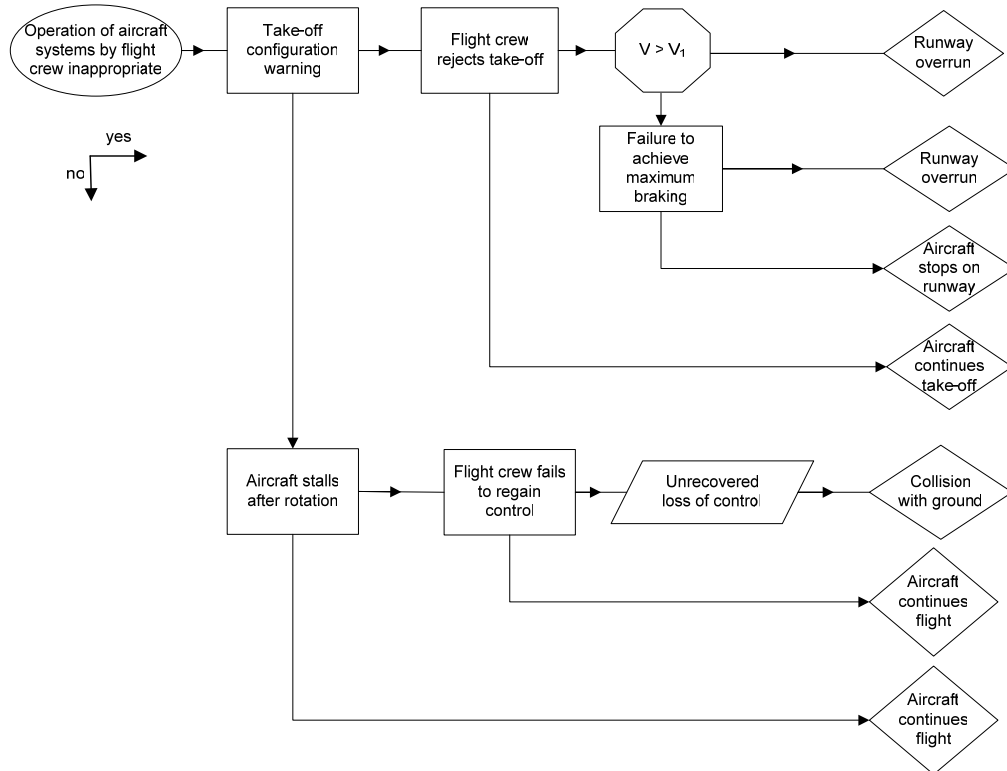


B.5 ESD 5

Accident type: uncontrolled collision with ground.

Flight phase: take-off.

Initiating event: Operation of aircraft systems by flight crew inappropriate.

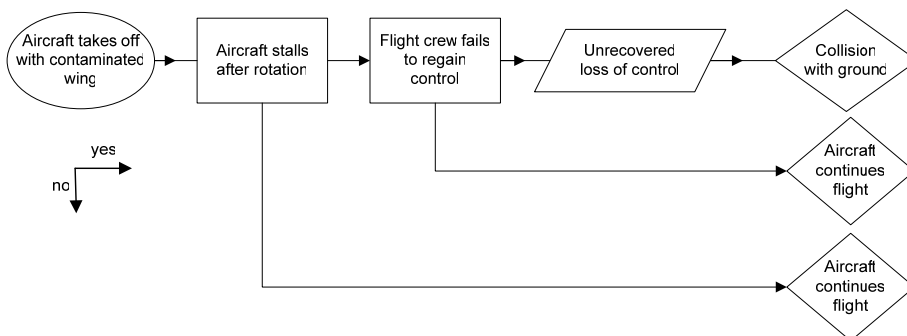


B.6 ESD 6

Accident type: uncontrolled collision with ground.

Flight phase: take-off.

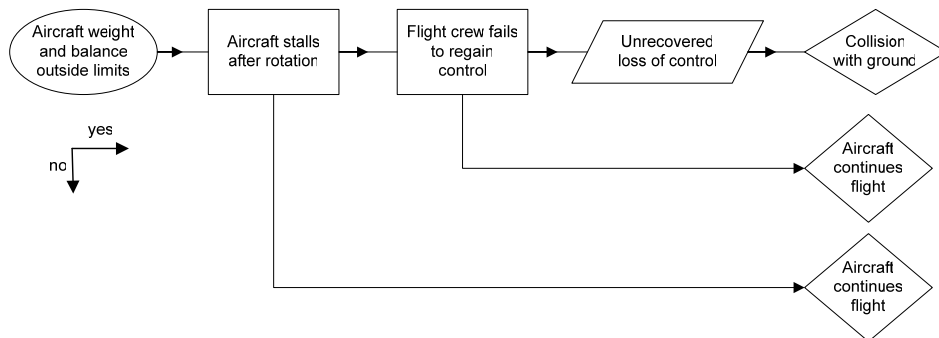
Initiating event: aircraft takes off with contaminated wing.





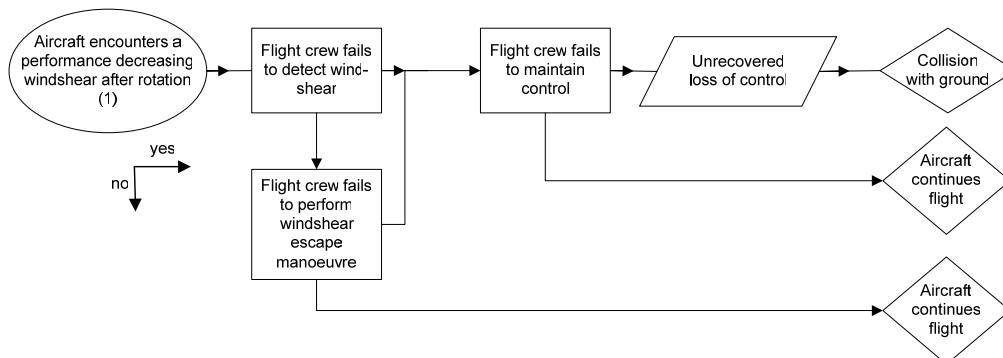
B.7 ESD 7

Accident type: uncontrolled collision with ground.
Flight phase: take-off.
Initiating event: aircraft weight and balance outside limits.



B.8 ESD 8

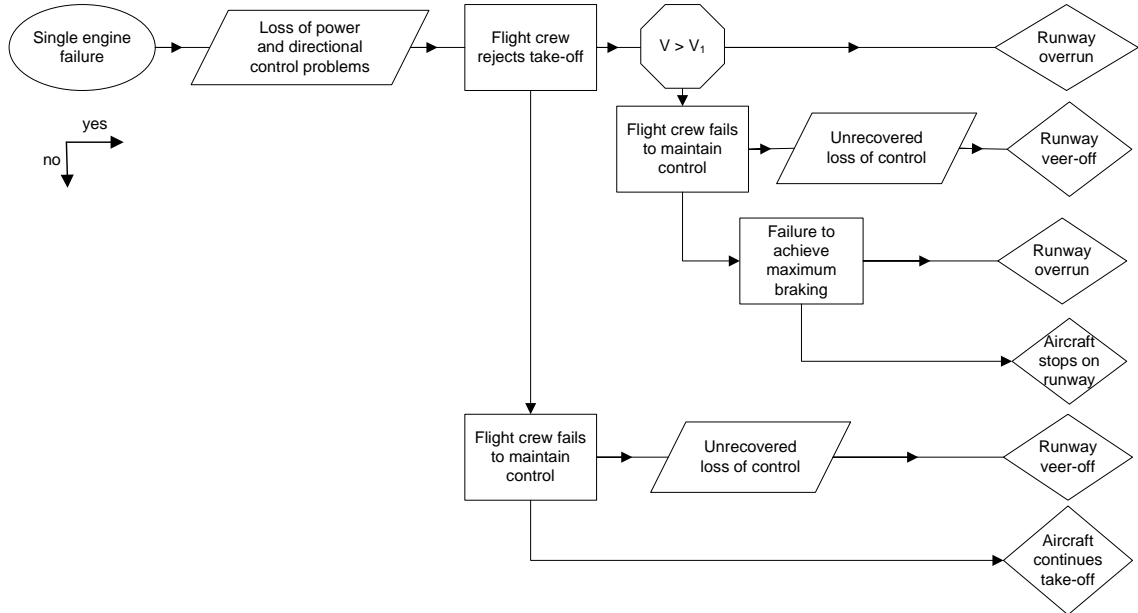
Scenario type: loss of control.
Phases: take-off.
Initiating event: aircraft encounters a performance decreasing windshear after rotation.



(1) Windshear is an abrupt change in wind direction and velocity. This ESD represents a situation where the aircraft encounters a performance decreasing windshear (decreasing headwind, increasing tailwind or a downdraft), e.g. as a result of a microburst.

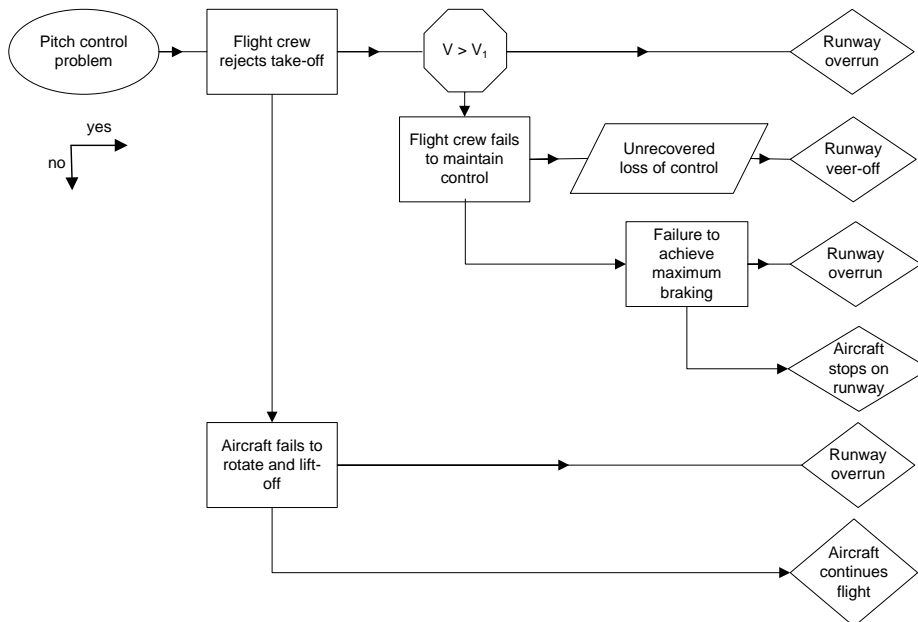
B.9 ESD 9

Accident type: uncontrolled collision with ground.
Flight phase: take-off.
Initiating event: single engine failure.



B.10 ESD 10

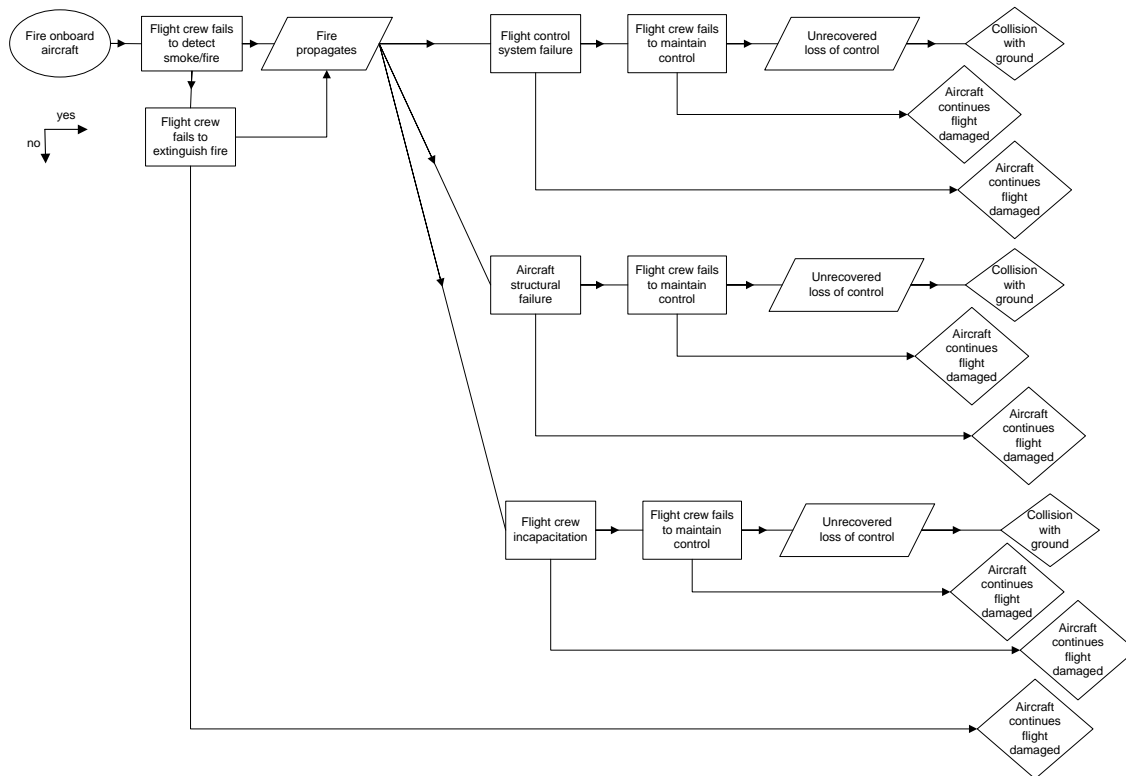
Accident type: uncontrolled collision with ground.
Flight phase: take-off.
Initiating event: pitch control problem.





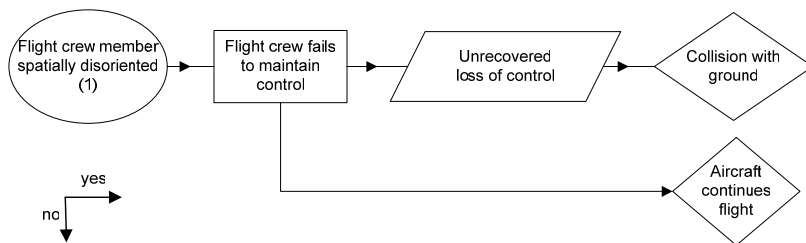
B.11 ESD 11

Accident type: fire/explosion.
Flight phase: take-off, initial climb, en route, approach, landing.
Initiating Event: fire onboard aircraft.



B.12 ESD 12

Accident type: uncontrolled collision with ground.
Flight phase: initial climb, en route, approach and landing.
Initiating Event: flight crew member spatially disoriented.

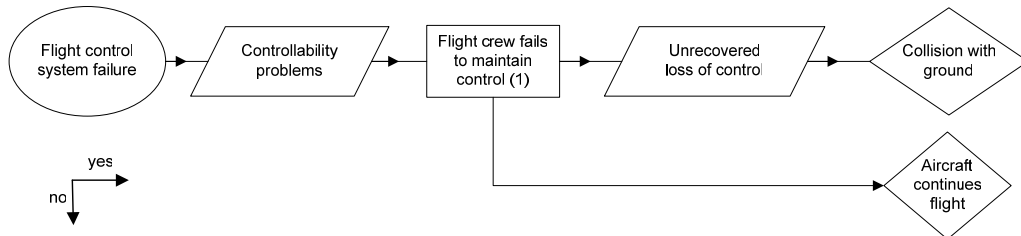


(1) Factors such as recognition of spatial disorientation, hand over of control to other crew member come under this event.



B.13 ESD 13

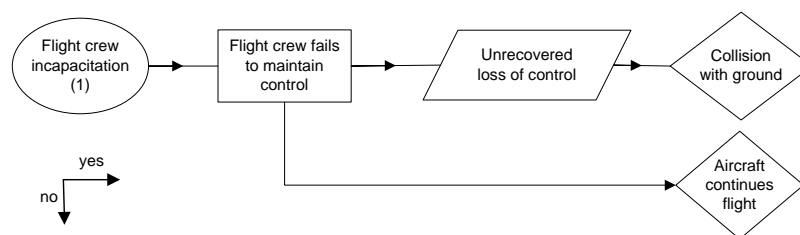
Accident type: uncontrolled collision with ground.
Flight phase: initial climb, en route, approach and landing.
Initiating Event: flight control system failure.



(1) Maintaining control is influenced by factors such as type of failure, crew response to the system failure, training, aircraft handling by crew etc

B.14 ESD 14

Accident type: uncontrolled collision with ground.
Flight phase: initial climb, en route, approach and landing.
Initiating Event: flight crew incapacitation.

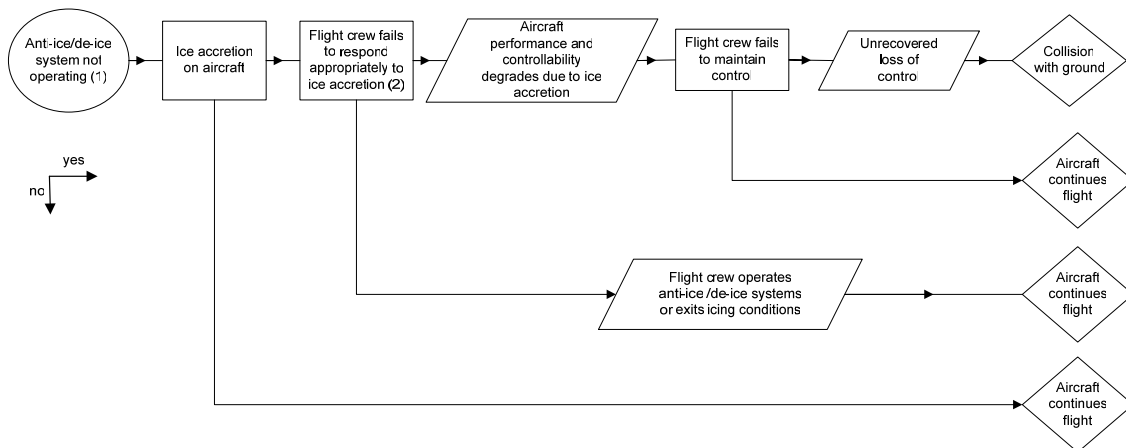


(1) Crew incapacitation can be the result of smoke, illness, depressurisation of cabin etc.



B.15 ESD 15

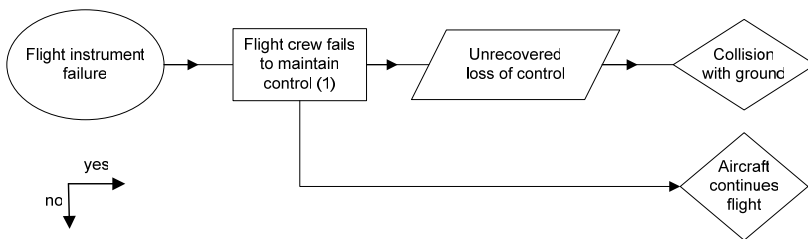
Accident type: uncontrolled collision with ground.
Flight phase: initial climb, en route, approach and landing.
Initiating Event: anti-ice/de-ice system not operating.



(1) 'Not operating' can be either a failure of the system or a failure of the crew to operate the system in icing conditions.
(2) This event may be influenced by ice detection by crew, crew awareness of hazards of icing conditions, training etc.

B.16 ESD 16

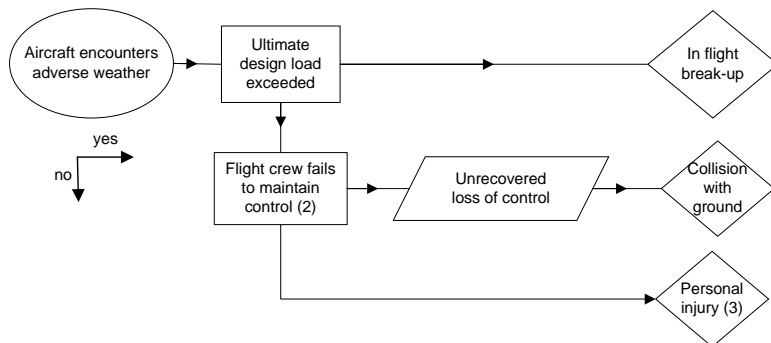
Accident type: uncontrolled collision with ground.
Flight phase: initial climb, en route, approach and landing.
Initiating Event: flight instrument failure.



(1) Inappropriate response to the system failure, training, monitoring flight path and instruments are factors which influence this pivotal event

B.17 ESD 17

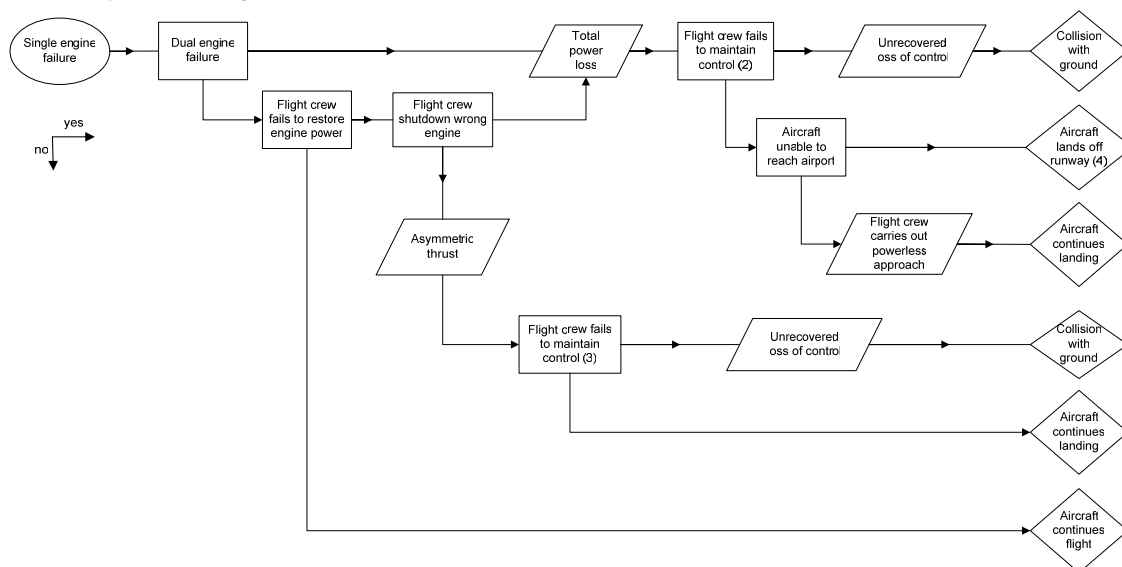
Accident type: structure overload
 Flight phase: initial climb, en route, and approach.
 Initiating Event: aircraft encounters adverse weather.



- (1) Aircraft response to adverse weather encounter (e.g. thunderstorm) may cause attitude, speed, altitude changes and accelerations.
- (2) This pivotal event represents also inappropriate upset recovery by crew.
- (3) Even if crew response to upset is appropriate passengers may be (fatally) injured or aircraft may be damaged, which is an accident by ICAO definition.

B.18 ESD 18

Accident type: uncontrolled collision with ground
 Flight phase: initial climb, en route, and approach.
 Initiating Event: single engine failure.
 Note: ESD represents twin engine aircraft.

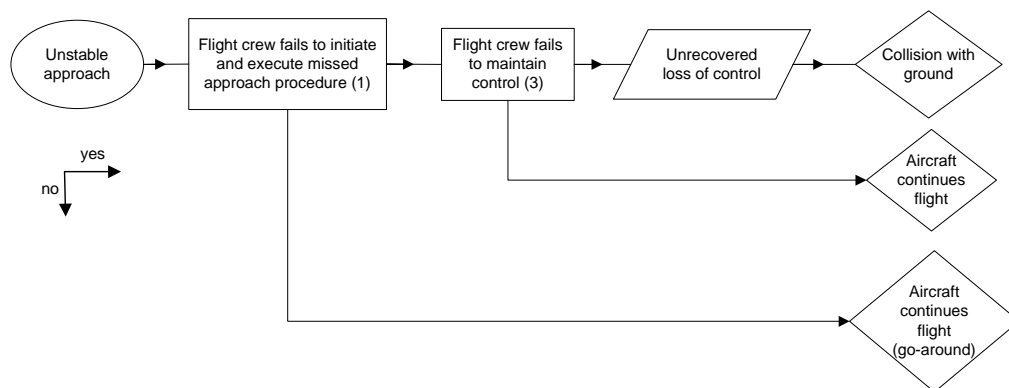


- (1) Asymmetric thrust due to an engine shutdown, feathered propeller or engine in idle thrust
- (2) This event incorporates control of speed, altitude, pitch and roll. Flight crew skills related to powerless flight
- (3) This event incorporates control of speed, altitude, pitch and roll, and power management. Flight crew skills related to one engine inoperative flight
- (4) 'Off runway' means a forced landing in field or ditching



B.19 ESD 19

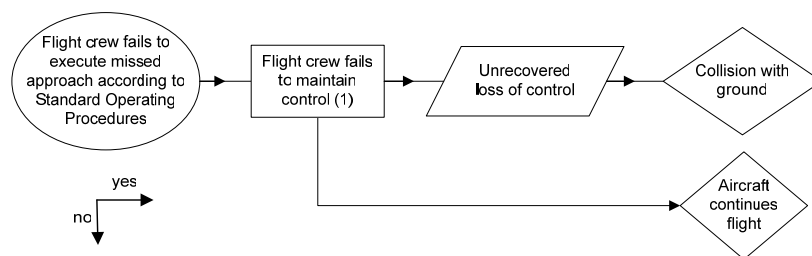
Accident type: uncontrolled collision with ground.
Flight phase: approach.
Initiating Event: unstable approach.



- (1) Crew Resource Management failure: crew fails to detect unstable approach and to take appropriate action
- (2) A continued unstable approach is also an initiating event for loss of control in the landing phase
- (3) Maintaining control is influenced by factors training, aircraft handling by crew etc

B.20 ESD 20

Accident type: uncontrolled collision with ground.
Flight phase: approach.
Initiating Event: flight crew fails to execute missed approach according to Standard Operating Procedures

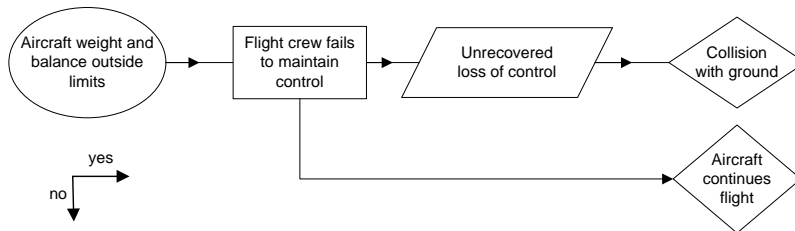


- (1) Maintaining control is influenced by factors such as training, aircraft handling by crew etc.



B.21 ESD 21

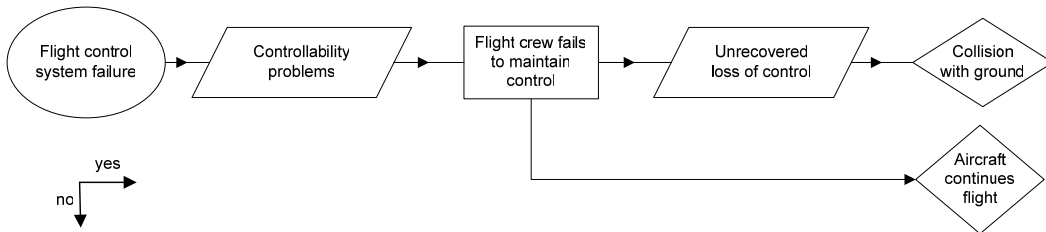
Accident type: uncontrolled collision with ground.
Flight phase: approach.
Initiating Event: aircraft weight and balance outside limits.



Note
Aircraft stall may occur during approach, for instance after a configuration change (flap selection)

B.22 ESD 22

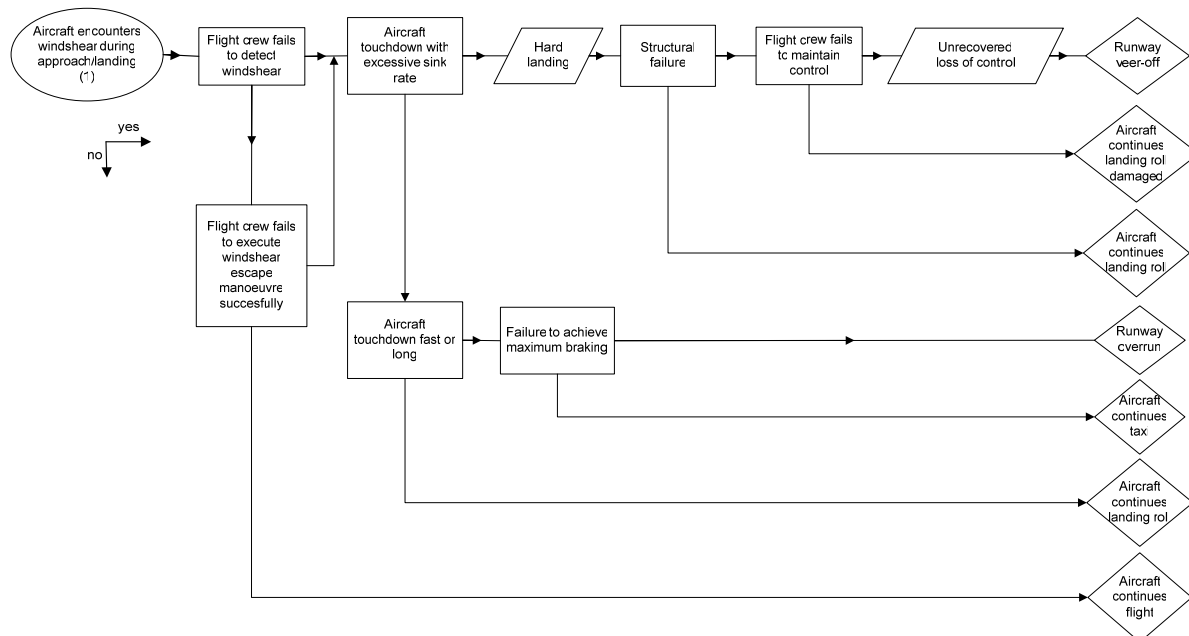
Accident type: uncontrolled collision with ground.
Flight phase: approach.
Initiating Event: flight control system failure.





B.23 ESD 23

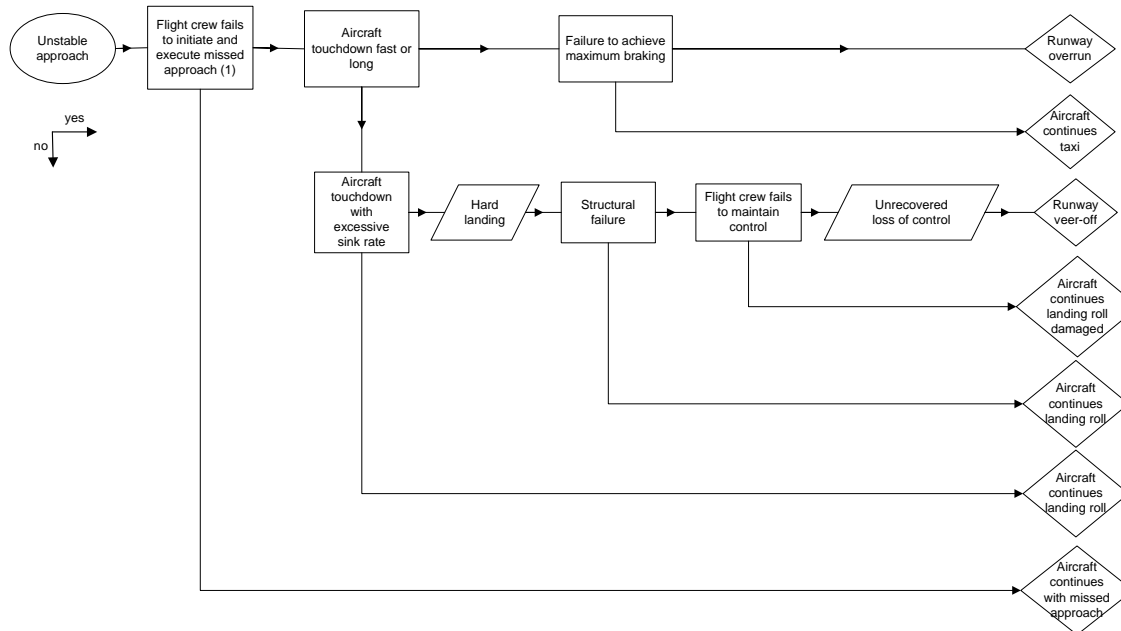
Accident type: uncontrolled collision with ground.
Flight phase: approach and landing.
Initiating Event: aircraft encounters windshear during approach/landing.



(1) Windshear is an abrupt change in wind direction and velocity. This ESD represents a situation where the aircraft encounters a performance decreasing windshear (decreasing headwind, increasing tailwind or a downdraft) or a performance increasing windshear (decreasing tailwind, increasing headwind).

B.24 ESD 24

Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: unstable approach.

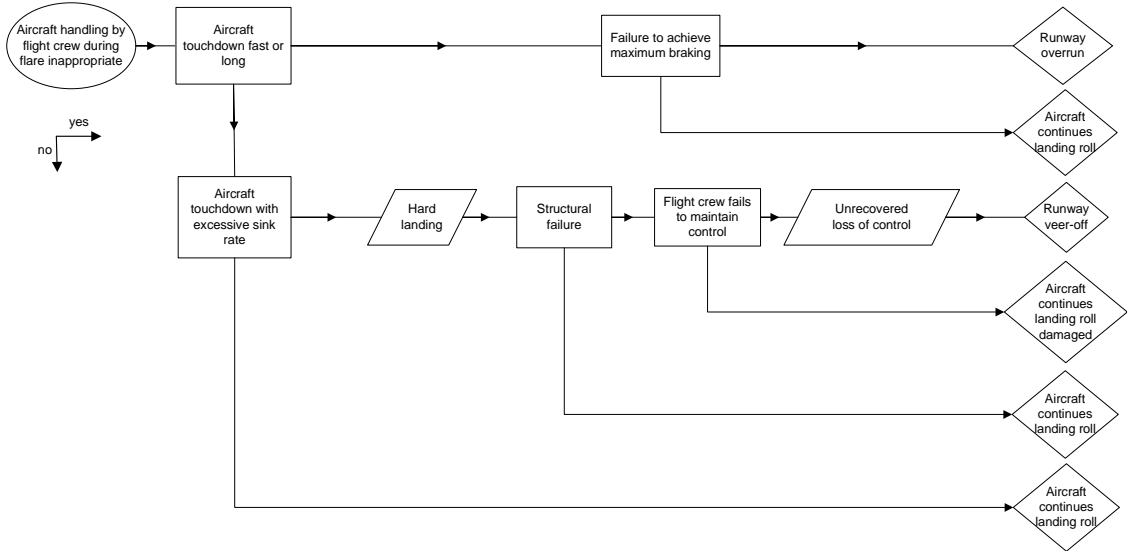


(1) Crew Resource Management failure: crew fails to detect unstable approach and to take appropriate action



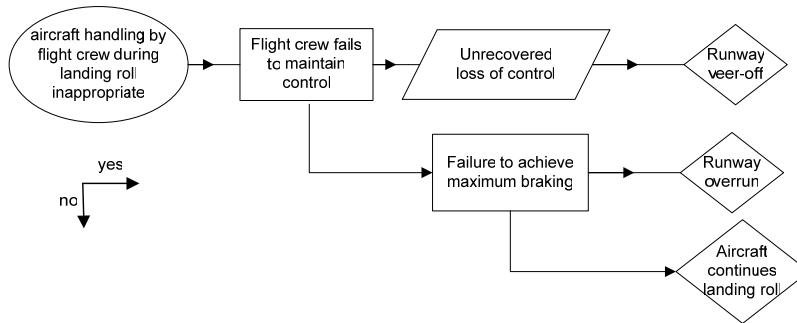
B.25 ESD 25

Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: aircraft handling by flight crew during flare inappropriate.



B.26 ESD 26

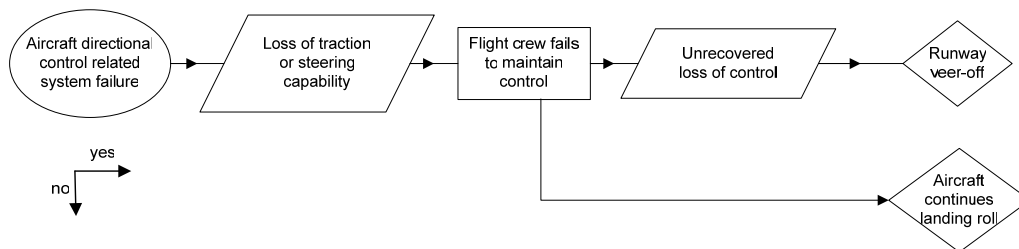
Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: aircraft handling by flight crew during landing roll inappropriate.





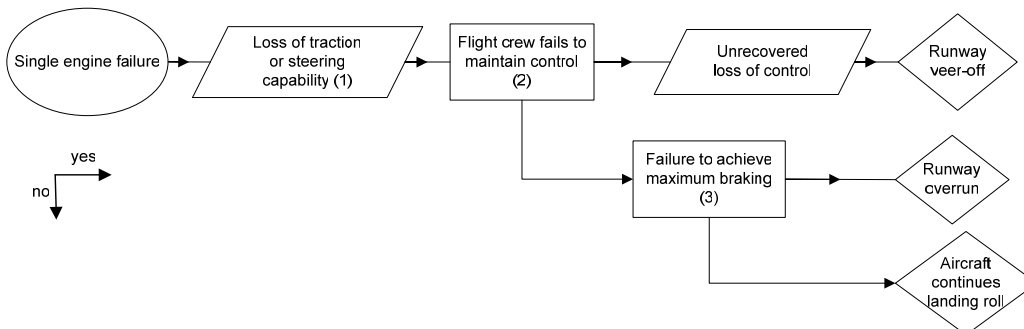
B.27 ESD 27

Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: aircraft directional control related system failure.



B.28 ESD 28

Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: single engine failure.

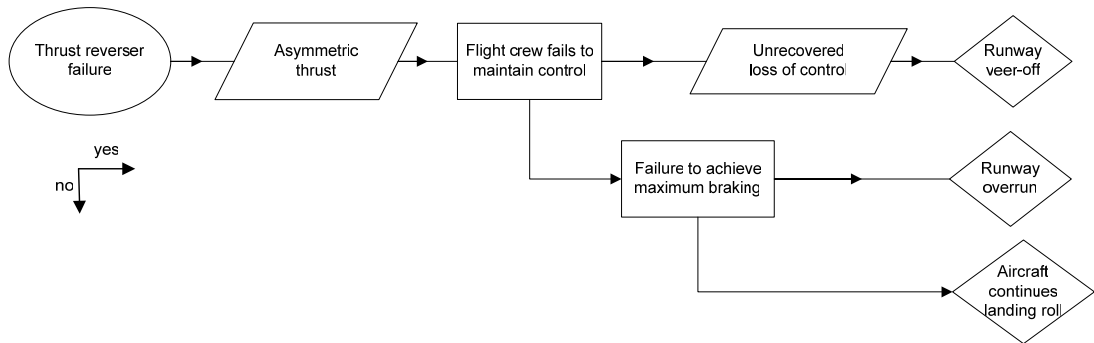


- (1) Asymmetric thrust may cause directional control problems.
- (2) Maintaining control is influenced by factors such as type of failure, crew response to the system failure, training, aircraft handling by crew etc.
- (3) Degraded stopping capabilities can be the result of crew controlling aircraft with rudder and manual braking simultaneously or dealing with positive thrust in roll out.



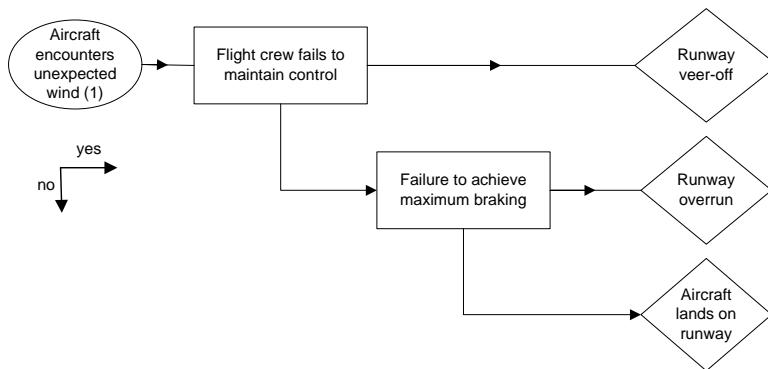
B.29 ESD 29

Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: thrust reverser failure.



B.30 ESD 30

Accident type: uncontrolled collision with ground.
Flight phase: landing.
Initiating Event: aircraft encounters unexpected wind.



(1) Unexpected wind (direction, strength) or wind is outside limits (tail, cross). This scenario applies when unexpected wind is encountered in landing and directional control problems occur. In case unexpected wind is encountered before the beginning of the flare the unstable approach scenario applies

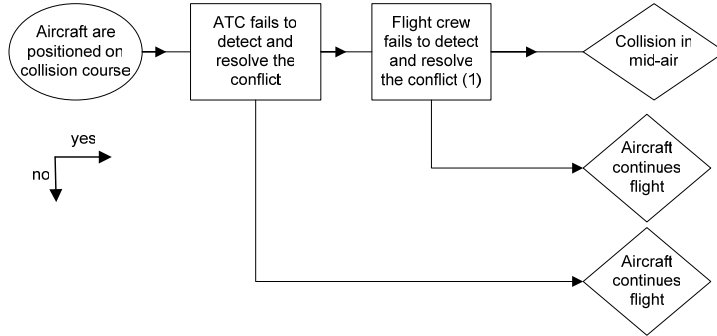


B.31 ESD 31

Accident type: mid-air collision.

Flight phases: initial climb, en-route and approach.

Initiating event: aircraft are positioned on collision course.



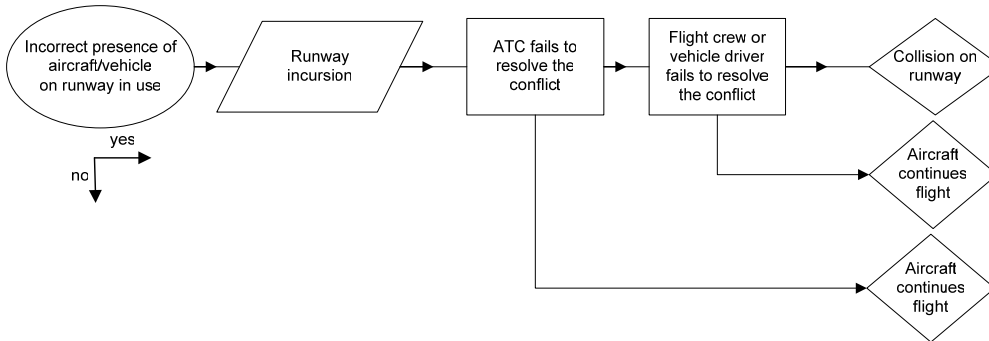
(1) This pivotal event includes the execution of 'see-and-avoid' principle and the response to a Traffic Collision Avoidance System alert.

B.32 ESD 32

Accident type: collision on ground.

Flight phases: taxi, take-off and landing.

Initiating event: incorrect presence of aircraft/vehicle on runway in use

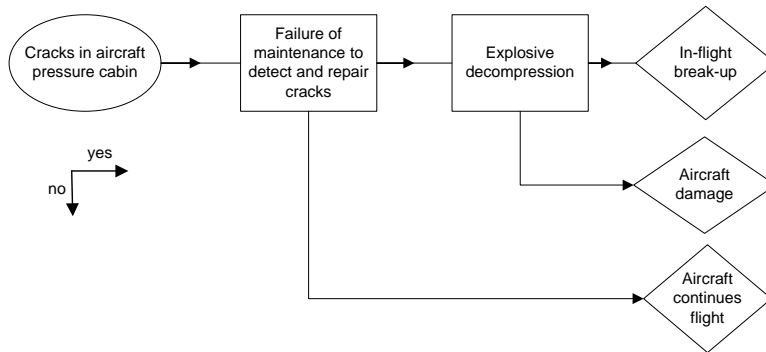


B.33 ESD 33

Accident type: structure overload.

Phases: take-off, initial climb, en route, approach and landing.

Initiating event: cracks in aircraft pressure cabin.

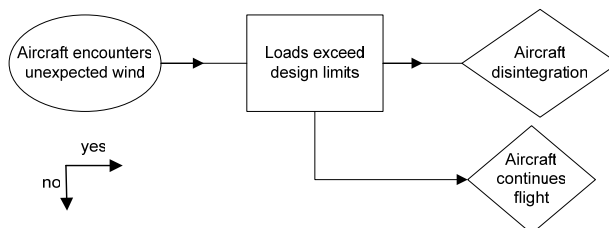


B.34 ESD 34

Accident type: structure overload.

Flight phases: take-off, initial climb, en route, approach, landing.

Initiating event: aircraft encounters unexpected wind.



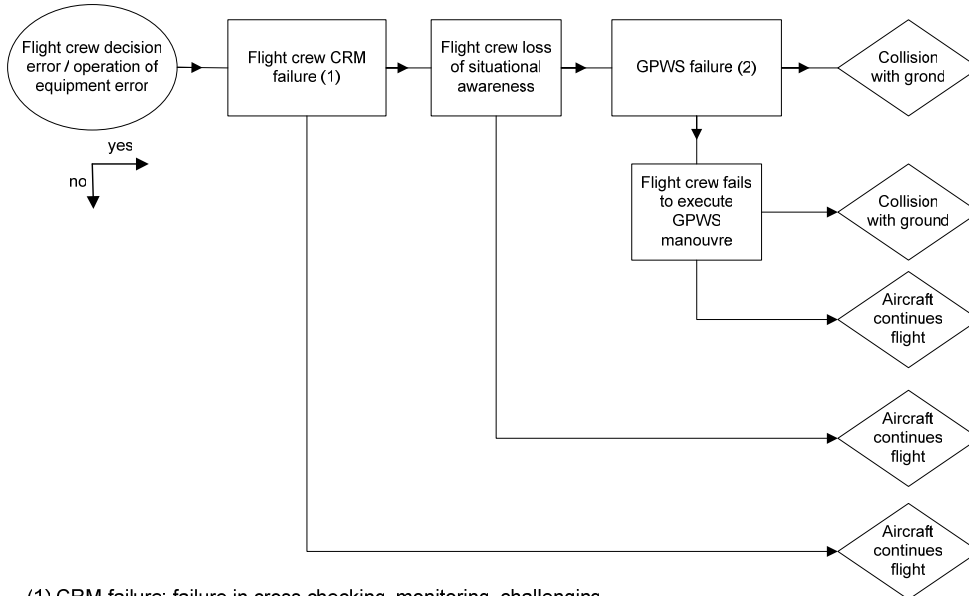


B.35 ESD 35

Accident type: controlled flight into terrain.

Flight phases: initial climb, en route, and approach.

Initiating event: flight crew decision error/operation of equipment error.



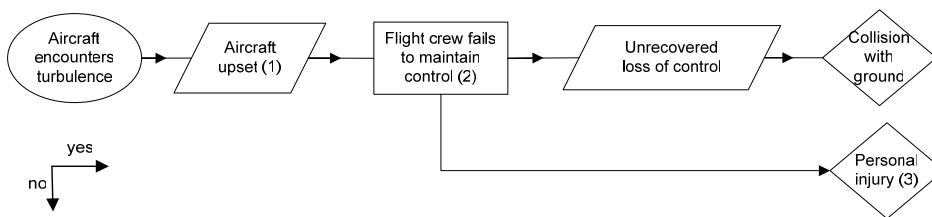
- (1) CRM failure: failure in cross checking, monitoring, challenging
- (2) GPWS not installed, early model or system malfunction

B.36 ESD 36

Accident type: abrupt manoeuvre.

Flight phase: initial climb, en route, and approach.

Initiating Event: aircraft encounters turbulence.



- (1) Aircraft response to turbulence encounter may cause attitude, speed, altitude changes and accelerations
- (2) This pivotal event represents also inappropriate upset recovery by crew
- (3) Even if crew response to upset is appropriate passengers may be (fatally) injured or aircraft may be damaged, which is an accident by definition



Appendix C Accident classification taxonomies

C.1 ICAO ADREP

In accordance with ICAO Annex 13 – Aircraft Accident Investigation, States report to ICAO information on all aircraft accidents which involve aircraft of a maximum take-off mass of over 2,250 kg. ICAO also gathers information on aircraft incidents considered important for safety and accident prevention. The ICAO accident incident reporting system is called ADREP (Accident/Incident Data Report), and instructions for its use are published as the ICAO Accident/Incident Reporting Manual (ADREP Manual), ICAO Doc. 9156-AN/900. The ADREP system is also used by the European Co-ordination Centre for Aviation Incident Reporting Systems (ECCAIRS). The objective of ECCAIRS is to integrate information from aviation occurrence reporting systems running in the authorities of the various EU member states.

In the ADREP system, the occurrence (accident or incident) is described by listing the ‘events’. The expression ‘phase’ is used to indicate in which phase of flight a certain event occurred and is always paired with an event. Additional ‘descriptive’ and ‘explanatory’ factors show why an accident or incident happened. To describe and explain the events, up to five descriptive factors can be entered for each event, with up to three explanatory factors for each descriptive factor. Descriptive and explanatory factors are combinations of ‘subjects’ and ‘modifiers’. The subject provides information on what was involved and the modifier gives the details. The ADREP manual lists approximately 260 different modifiers. Examples are ‘broken’, ‘degraded’, ‘eroded’, ‘failed’, etc. In addition to the coded information as described above, a narrative is part of the accident information in. The narrative provides a brief description of the accident, typically up to 200 words.

A big advantage of using the ADREP system is its completeness; virtually all possible accidents can be described. It is also standard ICAO language, which will facilitate acceptance by the aviation community. The level of detail that is provided in ADREP meets our purpose. An important characteristic is the categorization between system-related events and crew-related events, and the division between aircraft, ATM system and airport. Due to this categorization, interdependencies between different events are to a certain extent avoided, and this will be a big advantage once the individual events are further developed into fault trees.

C.2 EUROCONTROL HEIDI

The HEIDI (Harmonisation of European Incident Definition Initiative for ATM) taxonomy has a structure that is similar to ADREP. It was developed by EUROCONTROL as a harmonized taxonomy for ATM safety incident reporting.



C.3 NTSB

The US National Transportation Safety Board (NTSB) examines transportation accidents that have occurred in the USA or involved US vehicles. The aviation section of the NTSB investigates all aircraft accidents, tries to determine the probable cause and provides recommendations for the future.

To describe the accident, a 'sequence of events' is constructed as a list of occurrences with the associated phase of flight, similar to the ADREP system. Findings can be listed for each of the events to further detail what happened, using a three level structure of immediate, directly underlying and indirectly underlying factors. The findings are described as combinations of subjects, persons and modifiers.

C.4 CAST problem statements

The Commercial Aviation Safety Team (CAST) is a group of government and industry safety experts that was established to significantly lower the accident rate. CAST has chartered several working groups (called Joint Safety Analysis Teams JSATs) for a more in-depth analysis of the top accident categories; identification of "intervention strategies" for eliminating or greatly reducing such accidents; and prioritization and coordination of plans for implementing those strategies. JSATs were established for the most common types of accidents:

- CFIT
- Approach and Landing accidents
- Loss of control
- Runway incursion
- Turbulence.

As part of the analysis process, each JSAT developed a set of problem statements. These problem statements describe what went wrong, define a deficiency, or describe a potential reason why some action occurred or did not occur. Each JSAT used and built on the problem statements developed by previous JSATs. Consequently, a master file of almost 300 problem statements was established. All problem statements were subsequently analyzed and prioritized by a dedicated team of aviation experts [Problem Statement Analysis Process Report, February 23, 2001, Paul Russel & Jay Pardee].

The CAST set of problem statements, while extensive, was not developed in a systematic way. Nevertheless, CAST is well accepted and reflects significant 'brainpower' from a large group of aviation experts. Therefore the results from the CAST analysis, in particular the list of problem statements, should preferably be incorporated.



Appendix D ICAO accident definition

ICAO Annex 13 defines accident as follows:

Accident.

An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which:

- a) a person is fatally or seriously injured as a result of
- being in the aircraft, or
 - direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or
 - direct exposure to jet blast,

except when the injuries are from natural causes, self inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew: or

- b) the aircraft sustains damage or structural failure which:

- adversely affects the structural strength, performance or flight characteristics of the aircraft, and
- would normally require major repair or replacement of the affected component,

except for engine failure or damage. when the damage is limited to the engine, its cowlings or accessories: or for damage limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin: or

- c) the aircraft is missing or is completely inaccessible.

Note 1

For statistical uniformity only, an injury resulting in death within thirty days of the date of the accident is classified as a fatal injury by ICAO.

Note 2

An aircraft is considered to be missing when the official search has been terminated and the wreckage has not been located.



Incident.

An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation.

Note.

The type of incidents which are of main interest to the International Civil Aviation Organization for accident prevention studies are listed in the ICAO Accident/Incident Reporting Manual (Doc 9156).

Serious incident.

An incident involving circumstances indicating that an accident nearly occurred.

Note 1

The difference between an accident and a serious incident lies only in the result.

Note 2.

Examples of serious incidents can be found in Attachment D of Annex 13 and in the ICAO Accident/Incident Reporting Manual (Doc 9156).

Serious injury

An injury which is sustained by a person in an accident and which:

- a) requires hospitalization for more than 48 hours, commencing within seven days from the date the injury was received: or
- b) results in a fracture of any bone (except simple fractures of fingers, toes, or nose): or
- c) involves lacerations which cause severe hemorrhage, nerve, muscle or tendon damage: or
- d) involves injury to any internal organ: or
- e) involves second or third degree burns, or any burns affecting more than 5 per cent of the body surface: or
- f) involves verified exposure to infectious substances or injurious radiation.