Accident scenarios for an integrated aviation safety model

Roelen, A.L.C., Wever, R.
National Aerospace Laboratory NLR
P.O. Box 90502
1006 BM Amsterdam
The Netherlands

Paper presented at the 3rd International Conference
'Working on Safety',
12-15 September 2006, Zeewolde, The Netherlands

Abstract

In support of the Systems Approach to Safety Oversight (SASO) program, the US Federal Aviation Administration (FAA) has initiated research for the development of an integrated safety model. The proposed model architecture introduces a hybrid causal model of Event Sequence Diagrams, Fault Trees and Bayesian Belief Nets. The objective of this study conducted by NLR is the development of generic accident scenarios that are the upper layer of the hybrid model. The scenarios describe the combination of events that results in the transition of a hazard into an accident. The scenarios are simplistic. Despite this simplicity, the scenarios provide an appropriate framework for developing the underlying models. Because of the simplicity, the top layer of the integrated safety model is transparent and easy to understand.

Introduction

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. The US Federal Aviation Administration (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 aviation system [FAA 2004]. To meet this requirement, NLR participates in the development of an integrated risk model. A similar effort has been initiated by the Dutch Ministry of Transport [Ale et al 2005]. The proposed risk model architecture [Mosleh et al 2004] 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.

Aims

The proposed integrated methodology is intended to address multiple requirements and practical needs [Mosleh et al 2004], including identification and ranking of safety hazards and supporting risk-informed decision making.

The objective of this study conducted by NLR is the development of generic accident scenarios that are the upper layer of the proposed integrated safety model. The scenarios describe the combinations of events or conditions including the sequence of their occurrence that results in the transition of a hazard into an accident.

Methods

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. 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.

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. We propose to look at accident type and flight phase as main criteria for clustering accident scenarios.

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 term ‘accident’ is precisely defined by the International Civil Aviation Organization [ICAO Annex 13]. The accident categorization used in the present study is based on this ICAO definition. Accidents are accordingly further divided into subcategories ‘personal injury’ (including fatality), ‘aircraft destroyed’ and ‘aircraft damaged’, while three ways for an aircraft to be destroyed or sustain major damage are distinguished:

- Collision of aircraft with the ground
- Collision of aircraft with an object

- General disintegration of aircraft

Each of the main groups have been further subcategorized; The resulting set of accident archetypes is shown in Figure 1. 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.

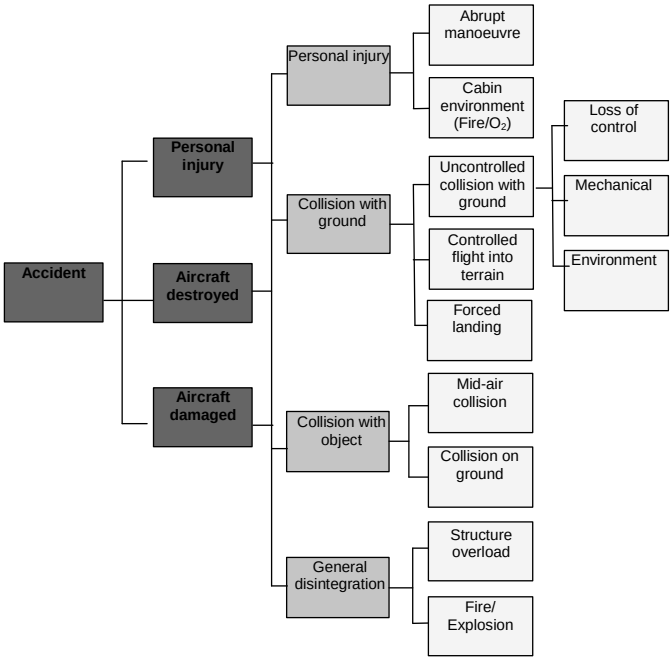

Figure 1: Accident categories

Definitions of each of the accident archetypes have been developed, taking into account existing definitions, in

particular the CAST/ICAO Common Taxonomy Team (CICTT) Aviation Occurrence Categories definitions [ICAO/CAST 2002, 2004].

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

Event Sequence Diagrams

An Event Sequence Diagram (Figure 2) 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].

By a suitable 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.

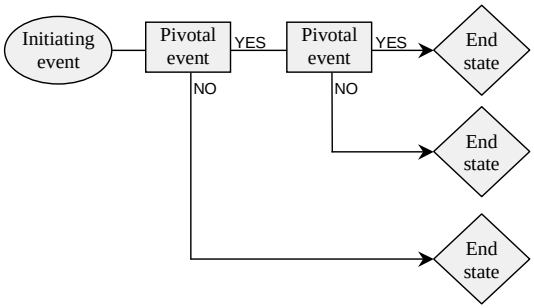

Figure 2: Event Sequence Diagram schematic

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.

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 deemed to have occurred. A physical parameters 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.

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.

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.

Pivotal events are not necessarily independent of each other. Indeed, in dynamic situations pivotal events can be 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.

Scenario development

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.

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.

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. 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 operators between 1994 and 2004.

Initiating and pivotal events of each individual accident were selected according to the criteria described above. 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.

Results

36 Event Sequence Diagrams with 29 different initiating events have been developed. An example is presented in Figure 3. This is the ESD for uncontrolled collision with terrain, flights phases climb, en-route and approach. The initiating event is single engine failure. A well-known accident that fits into this scenario is the Boeing 737-400 accident that happened near Kegworth on January 8, 1989 [AAIB 1990].

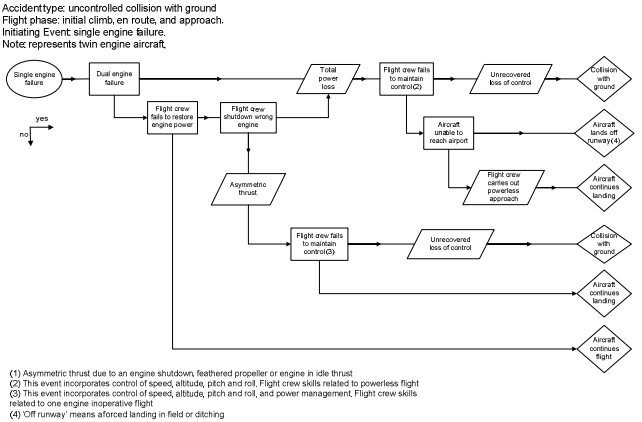

Figure 3: Example scenario

Design requirements for the scenarios include that they should serve as top-layer of the integrated safety model and can be used for communication. 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.

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. The main accident types have been defined based on the ICAO definition of an accident. Accident scenarios are grouped by accident type and phase of flight. 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.

The accident scenarios highlight the most important occurrences in the accident sequence of events. Underlying layers in the model will specify the causal pathways leading up to the events in the scenarios. As a result, the scenarios are simplistic. Despite this simplicity, the scenarios provide an appropriate framework for developing the underlying models. Because of the simplicity, the top layer of the integrated safety model is transparent and easy to understand.

References

Ale, B.J.M., Bellamy, L.J., Cooke, R.M., Goossens, L.H.J., Hale, A.R., Kurowicka, D., Roelen, A.L.C., Smith, E. 2005. Development of a causal model for air transport safety, Advances in safety and Reliability, Kolowrocki (ed), Taylor & Francis Group.

Aircraft Accident Investigation Branch, Report on the accident to Boeing 737-400 - G-OBME near Kegworth,

Leicestershire on 8 January 1989, Aircraft Accident Report No: 4/90 (EW/C1095), AAIB, Aldershot, UK.

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

Federal Aviation Administration. 2004. System Approach for Safety Oversight, Commercial Aviation, RE&D Requirements, version 7.0. FY2004-2006.

ICAO. 2001. Annex 13 to the Convention on International Civil Aviation, Aircraft Accident and Incident Investigation, Ninth edition, International Civil Aviation Organization, Montreal. Canada.

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

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

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.

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

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.

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