Development and Validation of a Comprehensive Hybrid Causal Model for Safety Assessment and Management of Aviation Systems

Alfred Roelen\textsuperscript{a}, Rombout Weyer\textsuperscript{a}, Ali Mosleh\textsuperscript{b}, and Katrina Groth\textsuperscript{b}

\textsuperscript{a}NLR Air Transport Safety Institute, Amsterdam, the Netherlands
\textsuperscript{b}Center for Risk and Reliability, University of Maryland, College Park, MD, United States

Abstract: The United States Federal Aviation Administration (FAA) has initiated the development of a causal risk model of commercial air transport in support of the System Approach for Safety Oversight (SASO) program. The model uses the so-called Hybrid Causal Logic (HCL) methodology which combines Event Sequence Diagrams (ESD), fault trees (FT) and Bayesian Belief Networks (BBN). The model is hierarchically structured: it includes 31 generic ESDs covering accident scenarios in various phases of flight at the top-level of the model, supported by numerous fault trees and BBNs to represent deeper causes of the ESD events. BBNs are used to extend the causal chain of events to potential human and organizational roots. Probabilities of the HCL models are obtained from extensive review and classification of commercial aviation accident/incident databases. A number of FAA operations research analysts, principal inspectors, and other experts actively participated in review and validation of the model development. A dedicated software prototype (IRIS) has been developed that simultaneously supports model development and model application.

Keywords: causal model, PRA, accident scenario, safety assessment

1. INTRODUCTION

An essential element of safety management is a system to achieve safety oversight. The 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 commercial air transportation system. In the context of this research a hazard is defined as an event or condition that could potentially lead to an unsafe outcome of accident scenarios. To meet the FAA research requirement University of Maryland, Hi-Tec Systems and the Air Transport Safety Institute of the Dutch National Aerospace Laboratory NLR have jointly developed a Hybrid Causal Model. The Dutch Ministry of Transport is developing a similar risk model to analyze risk reduction measures and to serve as a means of communication between experts and managers within the industry [1]. Because of the similarities between the two research efforts it was decided to frequently exchange results and if possible use similar components in the model and the model structure. This paper provides an overview of the FAA sponsored work which includes developing methods, risk models, and a software prototype.

2. MODEL ARCHITECTURE

The FAA requirement calls for a model that represents the aviation system in the area of operational functions and procedures as well as aircraft and equipment malfunctions, the organizational set-up (structure, policy, culture), human errors, environmental hazards (wind, turbulence, terrain), and contributory hazards (regulatory, system, economy). The requirement for completeness (system wide) and the potential complexity of the Hybrid Causal Model lead to the development of a hybrid model architecture [2]. The proposed risk model architecture is displayed in Figure 1. The proposed Hybrid Causal Logic (HCL) method extends the conventional risk analysis techniques, e.g. fault trees and event trees by introducing a hybrid causal model of Event Sequence Diagrams (ESDs), fault trees and influence diagrams. ESDs are used to define the context within which various causal factors would be
viewed as a hazard. A context is a combination of events or conditions including the sequence of their occurrence that results in the transition of a hazard to an accident; a context is 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 Networks (BBNs).

![Diagram of Hybrid Causal Model framework showing the ESDs on top, fault trees in the middle and the BBNs at the bottom.](image)

Figure 1: Hybrid Causal Model framework showing the ESDs on top, fault trees in the middle and the BBNs at the bottom.

3. MODEL ELEMENTS

3.1. Event Sequence Diagrams

ESDs represent generic accident scenarios in the Hybrid Causal Model. These scenarios typically represent active failures. The sequence of event starts from an initiating event, which can be regarded as a deviation from normal operation. The pathway follows through pivotal events, which represent ways to enter different pathways towards resolution or unsafe end states.

The term ‘accident’ is precisely defined by the International Civil Aviation Organization (ICAO). 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.

A review of accidents shows that often event sequences are very similar, even for cases where human error plays an important role in the accident sequence. An example of such a recurring accident type is an aircraft stall and loss of control following an attempt to take off while the aircraft’s wing is contaminated with snow or ice. Crash due to stall and loss of control following an attempt to take off with a contaminated wing in icing conditions can be considered an accident archetype. Another example of an accident archetype is a runway overrun following landing long and fast on a wet runway, possibly in combination with cross- or tailwind. A review of a large set of aircraft accidents
and incidents identified 31 of such accident archetypes [3]. These accident archetypes, represented as ESDs, provide a suitable backbone for the HCL model.

The scenarios describe 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 its top layer. In the development of the Hybrid Causal Model, we recognized it would be advantageous to use existing definitions or descriptions when defining initiating and pivotal events. Model acceptance by the FAA and 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.

3.2. Fault trees and Bayesian Belief Nets

Details in terms of the sequence of events that lead to the occurrence of the initiating and pivotal events are modeled in deeper levels of the model using a combination of fault trees and BBNs. These fault trees and BBNs describe the causal pathways and factors influencing the occurrence of the events in the ESD. The FAA, as primary user of the model, conducts oversight of airline operations, i.e. they oversee operational processes and do not directly influence the events in the ESDs. The inspection and oversight activities of FAA are taking place at the operational processes level, which is located deeper down in the model. The link between accident scenarios and operational processes is made through the fault trees and BBNs, and is required for application of the model. The concept of linking an ESD with fault trees and BBNs, and eventually with the operational and a FAA oversight/inspection process is shown in Figure 2. In this figure the ESD (blue), fault tree (orange) and influence diagram (light green) constitute the Hybrid Causal Model and are connected to the operational process (green) and inspection/oversight elements (yellow).

![Figure 2: Graph showing the link between the Hybrid Causal Model and the operational process and inspection/oversight elements.](image-url)
3.3. Flight Crew Operations Model

Human operator activities play an important role in accidents scenarios. We have developed a flight crew operations model, which is a quantitative model of flight crew operations to be connected with fault trees and ESDs, see Figure 3. Because the influences on human performance are generally ‘soft’ rather than deterministic cause-effect relations, the human operator is best represented by a BBN instead of a fault tree. The top event of the model is the node ‘flight crew decision or action error’, which has a probability expressed as ‘per flight’. The model nodes and their causal relationships have been quantified using a combination of data and expert judgment [4]. Quantified expert judgment was obtained from 5 experts according the method described in [5]. All experts are commercial airline pilots. The initial focus was to develop a practical and working model, ready for use within the HCL model. Consequently the model is relatively simple and some influences might require further refinement at a later stage.

![Figure 3: Flight crew operations model.](image)

3.4. Model Quantification

The objectives of the risk model require that the model can be used for probabilistic risk assessments. The probability of occurrence of the various accident scenarios must be expressed as a function of the initiating events. The ESD provides the qualitative description of the accident scenarios. It is quantified by assessing the probability of occurrence of each of the different pathways. The general approach was to quantify the probability of occurrence of the end states from accident and incident data and to quantify the initiating events with occurrence data such as an airline’s occurrence reporting system. Conditional probabilities of pivotal events were calculated from occurrence data and operational data or followed logically from the initiating event and end state probabilities. All probabilities are expressed in ‘per flight’.

For quantification of events in the ESDs, fault trees and BBNs different data sources have been used: accident and incident data, Air Safety Reports from airlines, Service Difficulty Reports from FAA, operational data (e.g. data on wind and runway conditions), and exposure data, i.e. non-accident data. The scope was limited to commercial fixed wing air transport with ‘western-built’ aircraft heavier than 5,700 kg. The time span covers 1990-2005. This period provided a dataset that is large enough for quantification and is considered representative for ‘current’ air transport. Because of the size of most databases involved, much of the initial analysis was done by running database queries, e.g. looking for particular key words. Each incident in the resulting dataset was then individually analyzed to verify whether it was applicable to the particular event under consideration. The primary source of data for
quantification of the probability of occurrence of the initiating event are the databases of Service Difficulty Reports and Air Safety Reports, but sometimes other sources of data were used if these were considered to be more accurate.

A difficulty of BBNs arises during quantification of the model. A combinatorial explosion threatens the assessment of probabilities. We have found a satisfactory way of dealing with this by deriving simplifying assumptions, which enables the quantification of the BBN with probabilities extracted from data [6]. The probability of occurrence of the input nodes are estimated from accident/incident data and operational data. The conditional probabilities have been estimated using a combination of data and engineering judgement. In the quantification of BBNs connecting to pivotal events, we have taken into account a) dependencies between the ESD events and the BBN, and b) the context of the ESD, e.g. landing or take-off phase [7].

4. VALIDATION

Model validation is a process of checking if the model provides a sufficiently correct description of the reality that it represents. Full validation would involve comparison of model results with reality for every possible set of conditions. For the HCL model that is considered here the number of possible conditions is so large that this is impossible. Therefore alternative methods for demonstrating the ‘validity’ of the model must be sought. Individual segments of the model with directly observable outputs will have to be validated, where ‘validation’ is restricted to a few specific conditions. Proof must be provided that the overall process for combining these segments into a single model is sufficiently correct and that this not only holds for the specific condition but also for other possible conditions. The hierarchical structure of the model is advantageous in this respect.

A comparison of take-off and landing overrun accident probabilities provides an example of checking the validity of the process of breakdown into different accident scenarios and aggregating the results. A runway overrun following an aborted take-off is an end state of ten different take-off accident scenarios in the model. Examples of these scenarios are attempted take-off with a contaminated wing or attempted take-off with the center of gravity too far forward. A runway overrun following landing is an end-state in eight different accident scenarios. Quantified model results are compared with three other research reports that contain estimates of the probability of occurrence of take-off overrun accidents or landing overrun accidents [8, 9, 10]. These studies had similar data inclusion criteria, although there are some differences in the time frame. Results of the comparison are presented in Table 1.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Take-off overrun</td>
<td>1.27 x 10^-7</td>
<td>1.36 x 10^-7</td>
<td>1.4 x 10^-7</td>
<td></td>
</tr>
<tr>
<td>Landing overrun</td>
<td>4.17 x 10^-7</td>
<td>3.87 x 10^-7</td>
<td>5.0 x 10^-7</td>
<td></td>
</tr>
</tbody>
</table>

The match between the model results and the other results is good and demonstrates that we have covered all relevant scenarios for take-off and landing overrun. All results are based on more or less the same data source and are in that sense not independent, but the comparison is important because it shows that indeed the process of breaking accidents down into generic accident scenarios and then aggregating the results is valid.

Further validation of the model was provided through an extensive review of model elements by FAA Operational Research Analysts, Principal Inspectors, and aviation safety specialists.
5. APPLICATION AREAS OF THE HYBRID CAUSAL MODEL

The Hybrid Causal Model can provide FAA and the industry with a common platform for safety assessment, with hazard assessment being one part, and can be used as a technical basis for risk-informed regulatory and oversight processes. In particular the Hybrid Causal Model can provide:

- A quantitative risk analysis platform for supporting risk-informed decision making, and for developing auditing tools, risk indicators and performance measures, diagnosis tools, strategic plans, and creation/removal of aviation regulations and guidance material such as Advisory Circulars (AC).
- A common language between aviation safety R&D, industry, and regulatory entities on issues of safety.
- A model-based hazard classification system by an organized representation of hazards in the form of ESDs, fault trees and BBNs.
- An environment for model-based inspection, event analysis, data gathering and analysis, and accident precursor analysis.
- An understanding of hazards and their cause-effect relationship.

6. DEVELOPMENT OF SOFTWARE TOOL

Besides the development of the actual, quantified causal models covering the aviation systems operations, the implementation of the Hybrid Causal Model required the development of mathematical algorithms dealing with combining influence diagrams and other causal modeling techniques. In addition to that, a software tool to provide the capabilities of the Hybrid Causal Model through user-friendly, application-specific functionalities was developed. University of Maryland developed a dedicated software prototype – Integrated Risk Information System (IRIS) – that simultaneously supported model development as well as model application. The Hybrid Causal Model, i.e. the set of ESDs, fault trees and BBNs, has been implemented in the IRIS software [11].

IRIS combines a user-friendly graphical interface with the computational engine that implements the Hybrid Causal Logic (HCL) algorithms [11] to solve risk models made of ESDs, fault trees (FTs) and BBNs. IRIS provides a framework to identify all risk scenarios and contributing events; calculates probabilities of the various risk scenarios (unique sequences of events and conditions leading to undesired events, i.e., accidents and incidents); ranks risk scenarios and risk contributors by their probabilities; and identifies the impact of specific changes. An overview of the IRIS platform is provided in Figure 4. The IRIS graphical user interface is divided into two main functions: modeling and analysis. The modeling functions allow the user to build and edit ESDs, fault trees (FT), and BBNs. The analysis functions produce cut-sets, importance measures, and risk indicators.

![Figure 4: IRIS software modules.](image-url)
Search, trace and drill down functions are provided in IRIS to facilitate navigation through the IRIS models. The user can navigate between the modeling and analysis functions by selecting from a set of tabs at the bottom of the screen. Using a highlighting function, the analyst is able to study the impact of specific events or factors with respect to one or more risk scenarios, e.g., all scenarios leading to a particular end state category. The HCL methodology is implemented in a powerful computational engine capable of solving large hybrid models of the size often seen in complex systems probabilistic risk assessments (as in nuclear power and space missions).

The HCL engine identifies risk “cut sets” and risk scenarios, and calculates the corresponding probabilities in an extremely fast and accurate manner. All IRIS features can be employed for a single risk scenario or a class of scenarios e.g., all of the scenarios leading to a particular category or type of end state.

IRIS also provides a capability for identification and ranking of a broad spectrum of hazards including those rooted in technical systems and its organizational and regulatory environment. IRIS also includes a risk indicator feature that allows the user to monitor system risk by considering the frequency of observation and risk significance of particular events (indicators) in the model.

7. CONCLUSIONS AND RECOMMENDATIONS

The Hybrid Causal Model is a prototype that has to be operationalized with operational expertise of typical users, such as FAA Operational Research Analysts (ORA) and Principal Inspectors (PI). One of the application areas of the Hybrid Causal Model is hazard identification and classification. ORAs and PIs can for instance use the model-based hazard classification system to map hazards on the Hybrid Causal Model, to track them in time, and to assess the associated risk. This evaluation allows model developers to identify the level of detail and scope required by the users for full-scale development. The full-scale Hybrid Causal Model will then serve as a comprehensive hazard classification and tracking system.

For further development into a practical tool the model should be linked directly with the data repository of inspection results, allowing analysis of the data via the model and feeding the model continuously with the latest data available.

The Hybrid Causal Model and the IRIS software extend the traditional risk modeling capabilities by including BBNs for representing the influence of social-economic and organizational factors on accident causation. From a research perspective further study into the modeling of such factors is needed. Areas of research could be: the necessity and feasibility of including social-economic and organizational factors in the Hybrid Causal Model, determining the influence of such factors on safety, and the modelling approach to capture them in the Hybrid Causal Model.

Acknowledgements
The work described in this paper was supported by the U.S. Federal Aviation Administration (FAA). The authors are indebted to the FAA for overall monitoring and coordination. The opinions expressed in this paper are those of the authors and do not reflect any official position by the FAA.

References


