Analysing Aviation Accidents using WB-Analysis
An Application for Multimodal Reasoning

Peter Ladkin, Karsten Loer
Technische Fakultät, Universität Bielefeld
{ladkin | karlo}@rvs.uni-bielefeld.de   http://www.rvs.uni-bielefeld.de

We describe our ongoing work in accident analysis. Accident reports should tell us at least what the accident was and what the critical events were. A third requirement they should fulfil is to *explain* these events (see below) and their sequence ($\rightarrow$temporal reasoning). Explanation concerns causes ($\rightarrow$causal reasoning), human intentions, purposes, capabilities and behavior (so-called *human factors*). Causality also involves the unfolding of events in time (*Explaining Failure in Tense Logic*, RVS-RR-96-13). We include social factors - obligations and the regulatory environment - amongst the human factors ($\rightarrow$deontic reasoning).

Reasoning about accidents: the basics

Formal reasoning about accidents involves addressing three basic issues:–

1. We must determine what to reason about (what's in the universe?).
   To do this in a formally correct way, we describe the world in the ontology of TLA, Lamport's Temporal Logic of Actions, because this ontology has shown itself sufficient for describing the temporal behavior of artifacts (process algebra & Petri net semantics use a similar ontology).
2. In principle, this should involve us in clarifying the relation between set theory (or other formal data structuring) and 'the world'. But we leave this to philosophers of mathematics. We're more interested in the accidents.
3. We must determine what kind of reasoning is involved.

Since a narrative is involved, tense logic (with the Kripke semantics) is an appropriate reasoning tool, given that the ontology has been declared suitable. We show that the ontology of TLA is sufficient for (A) description of machine behavior, (B) formulation of accident histories, and (C) determination of sequences of states leading to an accident. *States* are individuated by the collection of state predicates which are true in that state. This makes states into *types*. Particular occurrences of states can be identified by means such as timestamps or positions in the causal chain. States furthermore may have a duration. In contrast, *events* are particulars, representing specific changes in state. An individual event cannot recur, but its type (a TLA *action*) can be instantiated more than once. There are also *processes*, state/event mixes of bounded duration which describe undifferentiated actions. *Non-events*, the non-occurrence of awaited events, are also important (see below).

On closer inspection the logical operators in TLA are insufficient for adequate reasoning about accidents, so we extend TLA by introducing a *temporal point of view* (tpov), additional temporal operators ($[P]$,$\langle P\rangle$,$[F]$,$\langle F\rangle$) and additional rules (RVS-RR-96-13). We show that causal relations cannot be formalized by the $\rightarrow$ ("leads to") operator. Furthermore we draw the conclusion that causality cannot be a relation definable in tense logic (*Some Dubious Theses...*, RVS-RR-96-14).

How then to handle causality?

(See *Formalising Failure Analysis* RVS-Occ-97-06). The most appropriate semantics for our purpose is the Lewis criterion for causality (Lewis 1973). It is based on Lewis's formal semantics for counterfactual conditionals:– Let A and B be *events* or *state instances*. We define: *A is a causal factor of B* $\equiv$ *(A and B both occurred, and in the nearest possible worlds in which A did not happen, neither did B)*. This '*nearest possible world*' relation is Lewis's extension to Kripke semantics. Our conclusions from this part of the work are:

1. Lewis semantics is more easily seen as a relation of *causal explanation* rather than *causality*, since it includes purely logical notions (observe that *A is a causal factor of B* if *A is a logical consequence of B*); and an event may indeed have a singular cause, even though explaining why that event happened may require the invocation of many factors (Davidson 1967, Lewis 1973). So we call it a WB-analysis (for *Why..Because..*).
2. Use of the Lewis semantics leads us to the technical problem of handling *overdetermination*: the occurrence of two or more independent causal factors B and C for A that are individually sufficient
3. The Lewis semantics alone is sufficient to detect reasoning errors, as shown in several examples:
   (a) Cali:
   communication between crew and ATC as well as the ID/freq identity of ROZO and ROMEO shown to be causal factors

   (b) Warsaw:
   placement of the ridge and the runway surface shown to be causal factors

   (c) O'Hare:
   failure of the slat-retraction indicating system and the inability of the crew to observe the wing from the cockpit shown to be causal factors

   All these points, although occurring in the respective accident reports, were not cited as causal factors therein.
4. We have *complete* WB-analyses of the Cali, Warsaw and Nagoya accident reports.
5. WB-analysis successfully detects inconsistencies and highlights missing causes

Since the Lewis relation is binary, we represent results of the analysis in a graph whose nodes are events/states/processes, called the WB-graph (*Why..Because..*-Graph). We can determine the 'presence' of non-events in a WB-analysis by comparing the actual pattern of (occurring) events against rule-based 'standard operating procedures' (SOPs) (Palmer and Ladkin 19xx).

Is there more we can do? Refining WB-analysis

Aviation is strongly determined by regulations (FAR, ICAO stans, ...) and fixed behaviors (AIM, SOPs, ...). Standard operating procedures (SOPs) for pilots, airlines, ATC, FAA alike can be formulated as deontics. However, this highlights conflicting explanatory requirements!

As an example we use the recent Korean Air accident in Guam (*The Crash of Flight KE801...*, RVS-J-97-06):–

> On Wednesday 6 August, 1997 a Boeing B747-300 flew into terrain at night in rainy weather while approaching the Guam airport. The Lewis causality criterion determines the missing glideslope equipment, night, and weather conditions to be (actual) causal factors in the accident history. Analysed deontically, these factors in fact play no substantial role (assuming that weather is found to have been 'normally bad') since:
>
> 1. pilots and airline knew before the flight took off that glideslope guidance was unavailable, and that they the landing would use a different approach procedure. They chose to accept this constraint (deontic). All required systems for this different procedure were available and working (as far as we know).
> 2. the approach was designed for conditions of reduced visibility, including night and cloudy/rainy weather of the sort supposed to have been present on the occasion of the accident
> 3. the weather was not optimal, but it is not known to have played a significantly unusual role (cf windshear).
>
> Summary: The circumstances for the landing were generally known before start and with their decision to start, the CRW (and the airline) accepted them. Such deontic concerns take precedence in accident explanation over some purely physical factors such as the normal circumstances of landing.

The importance of the deontics is emphasised by (Reason 1989):

> Data from the Institute of Nuclear Power Operations (INPO) shows that 92% of errors were man-made; that only 8% of the total were initiated by the operators. "The majority had their origins in either maintenance-related activities, or in fallible decisions taken within the organisational and managerial domains" (Reason 1989). These are the 'latent errors'. The Australian BASI uses Reason's latent-error model for all flight accident reports (Reason 1990).

We conclude that deontic reasoning introduces knowledge/a point of view that takes explanatory priority over (physically) causal factors which do not fit in with the regulatory environment (formulated as obligations). Furthermore, deontic and causal reasoning interacts incompatibly - but we lack an explanation of how!

Closed World Assumptions and other Non-Monotonicity:

CWA: Accident reports use a closed-world assumption, namely that either all the significant events and states are known, or those that are not known are known to be not known. Both the CWA and other non-monotonic reasoning can be expressed in the ontology introduced above.

...and other Non-Monotonicity: In principle, the 'world' consists only of states or events obtained *directly* from instruments like cockpit voice recorder (CVR) and digital flight data recorder (DFDR, 'black box'); photographs; on-site investigation of wreckage; states, events or processes derivable by temporal, causal and deontic reasoning from these. Formally, for every 'new' node (representing new knowledge of one of these states, events or processes) we introduce in our analysis, we have to check whether former reasoning is still valid (there are thus two cases: simple incompleteness and non-monotonicity - see below). Whenever we make an *assumption* about a cause for a state/event/process, we limit the explanatory power of the system to explanations which fulfil this assumption. To keep this limitation within bounds (we prefer to base analysis on formal argumentation rather than speculation), it would make sense formally to clone the 'existing' world before we introduce the new information, as in the method of semantic tableaux. We would need to control the potential exponential growth of the number of worlds to consider. Alternatively, we can be content with justifying 'reasonable' assumptions and ignore alternatives, but we may have to be prepared to revise these in light of further discovery (non-monotonicity). Examples:–

Cali (incompleteness, monotonic reasoning):
DFDR recordings show that the machine turned left for 90 seconds. This could not be explained, until an undamaged FMC was discovered and its non-volatile memory decoded. In this case, the WB-method would yield an incomplete, but causally correct graph, which contains all information discovered, but not including grounds for the left turn. The additional information gleaned from the FMC several months after the accident can be introduced to 'complete' the graph. Such 'completions' result in addidtional subgraphs, but do not change the rest of the graph.

Lauda Air, Thailand (assumption, non-monotonic):
Evidence from CVR that reverse thrust (RT) was 'deployed'; but there's an interlock.
Conclusion: upset cannot be directly explained. Subsequently found a failure mode of the interlock, which in principle could allow RT to actuate in flight. Report contains no probable cause, but considers this to be a likely scenario.

Mont Ste. Odile, Strasbourg (assumption, non-monotonic):
Autopilot modes not available on DFDR; flight path shows rapid descent starting exactly at FAF. Descent rate in fpm is almost identical with required flight path angle in degrees; also the autopilot descent mode would have been engaged at FAF, where divergent behavior started. Autopilot mode control is unlabelled toggle; mode annunciation is via small letters, rate/angle larger figures. Again, this 'likely cause' is presumed.

Summary: All accident reports make a CWA: the relevant facts are those we know plus those we know we don't know. Assumptions about 'likely happenings' introduce either an extra (formal) modal dimension or non-monotonicity.

Conclusions: Multimodal reasoning is essential for formal analysis of accidents:

Method	Used for:
modal logic/Tense Logic	temporal reasoning
Lewis counterfactuals augmented 'Kripke' semantics	causal explanation
deontic reasoning	incorporation of SOPs incorporation of regulatory environment incorporation of significant non-events reasoning about 'latent' errors

References

Davidson 1967 D. Davidson, *Causal Relations*, Journal of Philosophy 64:691-703, 1967.

Lewis 1973 D. Lewis, *Causation*, Journal of Philosophy 70:556-67, 1973.

Palmer and Ladkin 19xx E. A. Palmer and P. B. Ladkin, *An Analysis of "Oops"*, NASA ARC and RVS-??, to appear.

Reason 1989 J. T. Reason, *The contribution of latent human failures to the breakdown of complex systems*, in *Human Factors in Hazardous Situations*, ed. D. E. Broadbent, A. Baddeley and J. T. Reason, Oxford U. P., 1989.

Reason 1990 J. T. Reason, *Human Error*, Cambridge U. P., 1990.

RVS-** Publications in `http://www.rvs.uni-bielefeld.de`