Airbus A320 Braking as Predicate-Action Diagrams

Peter B. Ladkin
Universität Bielefeld, Technische Fakultät
Postfach 10 01 31, D-33501 Bielefeld
ladkin@techfak.uni-bielefeld.de
http://www.techfak.uni-bielefeld.de/~ladkin/

Abstract

We use the Predicate-Action Diagrams of Lamport to express the description of the operation of the Airbus A320 braking systems contained in the Flight Crew Operating Manual. This helps identify ambiguities and incompleteness.

1 Introduction

On September 14th, 1993, a Lufthansa Airbus A320 landed at Warsaw Airport in Poland in a thunderstorm. It overran the end of the runway, surmounted an earth bank, and came to rest on the other side. Two people died and others were injured in this accident, which began to interest us and others in the design of the A320 braking system [FI.93a, FI.93b, FI.93c]. This paper analyses the specification of the A320 braking system contained in the Flight Crew Operating Manual [FCOM], and rewrites it in Predicate-Action Diagrams of Lamport [Lam94b]. A fuller version of this work containing an analysis is [Lad95].

Flight crew should have a complete, accurate high-level specification of system operation from which to work. This may be provided using predicate-action diagrams, with advantage over the Boolean logic expressed in English that is currently used. This is in line with current thinking, for example by the task force studying controlled flight into terrain – "a factor that often crops up when crashes are analysed is the failure of the pilot at the controls to stick to standard flight procedure. But that is not necessarily the pilot's fault: [...] Or perhaps poor descriptions mean the procedure is misunderstood." [Eco94].

The Braking System Design of the A320. The braking system design of the A320 is described in the A320 Flight Crew Operating Manual [FCOM]. There are four main components of this system, of which the two primary components are the brakes and anti-skid. The other two are the spoilers (which destroy lift from the wings) and the thrust reversers (which divert engine exhaust to thrust in a forward direction). The brakes and anti-skid system are described in [FCOM, 1.32.30: Landing Gear: Brakes and Anti-Skid]; the spoiler activation in [FCOM, 1.27.10: Flight Controls Description, P11]; the thrust reverser actuation in [FCOM, 1.70.70: Power Plant: Thrust Reverser System].

Predicate-Action Diagrams and TLA$^+$ Specifications. A predicate-action diagram is a simple state diagram in which the states are given by the values of chosen *state predicates* (conditions which have values), and transitions between these states, indicated by labelled arrows, are actions of a given type. Predicate-action diagrams corresponding to the braking system descriptions are shown in Figures 1, 2 and 3. Predicate-action diagrams have a simple formal translation into the temporal logic TLA [Lam94a].

Related Work. The Airbus approach to using computers in civil aircraft design is presented in [Pot93]. Much fundamental research and analysis of algorithms involved in flight control and management stems from SRI Computer Science Lab, and may be found on the WWW starting at `http://www.csl.sri.com/ft-history.html` . A comprehensive introduction to safety analysis for systems involving computers in general is [Lev95]. Aircraft engineering safety issues are discussed in [LT82]. Standards for certification of flight-control systems are in [RTCA92].

Analysis and statistics of airplane accidents appear in [OSZ92]. Articles concerning the DC-10 accidents appear in [FB92]. An account of fatal A320 accidents to date is in [Mel94]. Reports of facts and findings related to the Warsaw accident are in [FI.93a, FI.93b, FI.93c], and the official report on the Warsaw accident itself is [MCAAI94].

2 The Design of the A320 Braking System

The braking system design of the A320 is described in the A320 Flight Crew Operating Manual [FCOM],repeated in [Lad95]. We give some sample entries. Each page is identified by a section number (three sets of digits separated by periods), a *REV*ision number, a *SEQ*uence number, and a Page number.

Landing Gear: Brakes and Anti-Skid (1.32.30)

1.32.30, REV 16, SEQ 001, P 1

[...]

Anti Skid System

[...]
The anti skid is deactivated when the speed is lower than 20 kts (ground speed). An ON/OFF switch activates or deactivates the anti skid system and nose wheel steering.

Principle

The speed of each main gear wheel (given by a tachometer) is compared with the aircraft speed (reference speed). When the speed of a wheel decreases below 0.87 time [*sic*] reference speed, brake release orders are given to maintain the wheel slip at that value (best braking efficiency).

1.32.30, REV 15, SEQ 001, P 3

Auto Brake

System arming

The crew may arm the system by depressing the LO, MED or MAX push button switches, provided all the following arming conditions are met:

- Green pressure available
- Anti-skid electrically powered
- No failure in the braking system

Note: *Auto brake may be armed with parking brake on.*

System Activation

Automatic braking is initiated by the ground spoiler extension command (refer to 1.27). Consequently in the event of an acceleration stop, if the deceleration is initiated with the speed below 72 KTS, the automatic braking will not be operative because the ground spoilers will not be extended.

System disarming

The system is disarmed by:

- Pressing the push-button switch or,
- Loss of one or more arming conditions or,
- Applying sufficient force to the rudder pedals when autobrake is operating:
  - In MAX mode both pedals must be depressed,
  - In MED or LO desarming [*sic*] may be accomplished by action on one pedal only,
- Ground spoiler retraction (refer to 1.27).
- Flight condition since 10 seconds.

1.32.30, REV 15, SEQ 001, P 4

[...]

Normal Braking

Braking is normal when:

- green hydraulic pressure is available
- A/SKID and N/W STRG is ON
- PARKING BRAKE is not ON.

Anti-skid is operative and autobrake is available.

The control is electrically achieved through the BSCU:

- either via the pedals
- or automatically
  - on ground by autobrake system
  - in flight by setting the landing gear lever to the up position

Anti-skid system is controlled by the BSCU via the normal servo valves.
No brake pressure indication is provided.
[...]

Flight Controls Description (1.27.10: REV 18, SEQ 106, P 11)

Ground Spoiler Control

Achieved by the spoilers 1 to 5.

- **Ground spoilers are armed** when the speed brakes control lever is pulled up into the armed position.
- Ground spoilers automatically extend:
  - (At MLG touch down) OR (During T.O run at speed greater than 72 KT)

    WHEN
    - (They are armed and all thrust levers are at idle) OR
    - (When reverse is selected on at least one engine (remaining engine at idle)
- Ground spoilers retraction is achieved when:
  - (All thrust levers are set at idle) AND (Speed brake control lever is pushed down)

    OR
  - One thrust lever advanced
    - above 20°
    - at least 3 sec between 4° and 20°

3 Analysis and Critique

The specification of the braking system design includes some causal or temporal dependencies, as well as specifying state changes, thus ensuring that Boolean logic must be supplemented by a semantics that considers change over time, hence our preference for TLA. In the semantics of TLA, a collection of Boolean values of the propositions describes a *state*. A proposition is a *state predicate*, since its Boolean value depends on the state in which it is evaluated. A logical formula describing how a state changes is called an *action*.

Real-time constraints also appear essentially in the FCOM description, e.g.: *The system is disarmed by: [...] flight condition since 10 seconds. Ground spoilers retraction is achieved when: [...] at least 3 sec between* 4° *and* 20°. They may be handled in TLA [AL94], but we don't attempt that here. In [Lad95], we identified the following problems with the descriptions:

ambiguities due to imprecise statement, or to infelicitous phrasing in English;

confusion between action and state: a desired result is achieved when, e.g. *[X] occurs when [Y] is activated*, or *[X] occurs when lever [Y] is pulled up.* Do the conditions on *[Y]* refer to its state, or to an action performed on *[Y]*? Whether certain states are acceptable or anomalous may depend on which reading is given;

imprecision in stating Boolean conditions: potentially ambiguous English descriptions are used to represent Boolean expressions, especially since parentheses are not included. However, in at least one place, an accurate Boolean formula is used. Pilots are clearly expected to understand Boolean formulas;

multiple terms used for a single concept or value: for example *insufficient* pressure, or *low* pressure; such terms are rarely noted to be synonyms;

incorrect mathematics is used in one place to describe a crucial quantity–an integral should be used, but does not appear.

4 The FCOM Specification as Predicate-Action Diagrams

We use predicate-action diagrams to represent the information contained in the specification. Predicate-action diagrams are almost self-explanatory. The nodes are partial states, that is they are collections of values of selected state predicates. We call these partial states 'states'. 'Actions' change the values of the state predicates, and are represented by arrows between the 'states'. The 'actions' represented in the diagrams are collections of *all* the actions that can change the value of one of the predicates of the 'state'. It is required that the result of any action that changes the value of the 'state' belongs to one of the 'actions', and that all the 'states' that result from any of the actions belonging to an 'action' appear in the diagram. Thus, a predicate-action diagram focuses on certain predicates, and shows how the values of those state predicates are changed by actions of the system, which are grouped into sets of actions that all have the same effect on the selected state predicates.

In the representation of the FCOM specification in predicate-action diagrams, we represent the 'actions' by logical disjunctions of its component actions. We also label the 'states' by certain useful indicative expressions. Thus, a braking-mode 'state' labelled with *normal* satisfies the state predicate that *braking-mode = normal*. However, these labels, while helpful, do not necessarily correspond to explicit state predicates. The state predicates explicitly asserted in the 'state' are given by conjunctions written in an ellipse attached by a line to the 'state'.

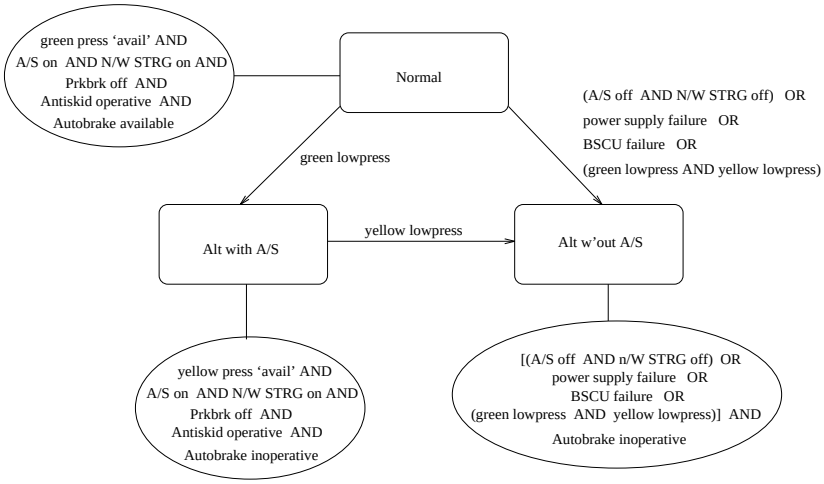

Figure 1: The Braking Modes from the FCOM Specification

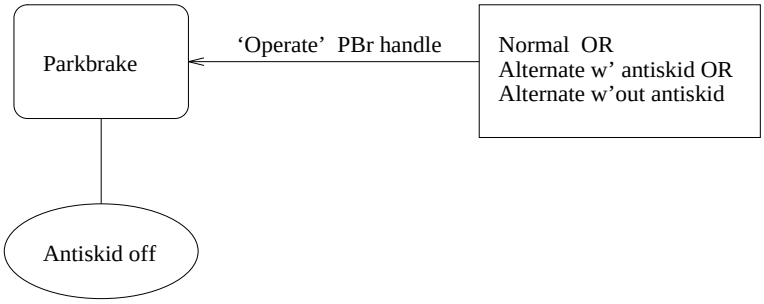

Figure 2: The Parking Brake Mode from the FCOM Specification

We omit the predicate-action diagram corresponding to the thrust reverser system, because it is not revised when we apply our rewriting criteria.

5 Revising the Predicate-Action Diagrams

The predicate-action diagram representation of the FCOM description can easily be completed, in the following steps:

- list all state predicates occurring in any diagram;
- determine the values of all the state predicates in every state denoted, and list them with the state;
- add transitions each way between all pairs of states;
- notate each transition with its action description (where possible);
- disambiguate the action descriptions from a given state (if necessary);
- note those transitions between pairs of states that cannot occur, and remove these transition arrows.

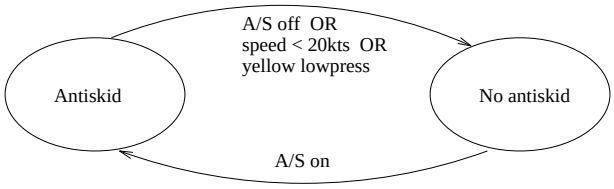

Figure 3: The Antiskid Condition from the FCOM Specification

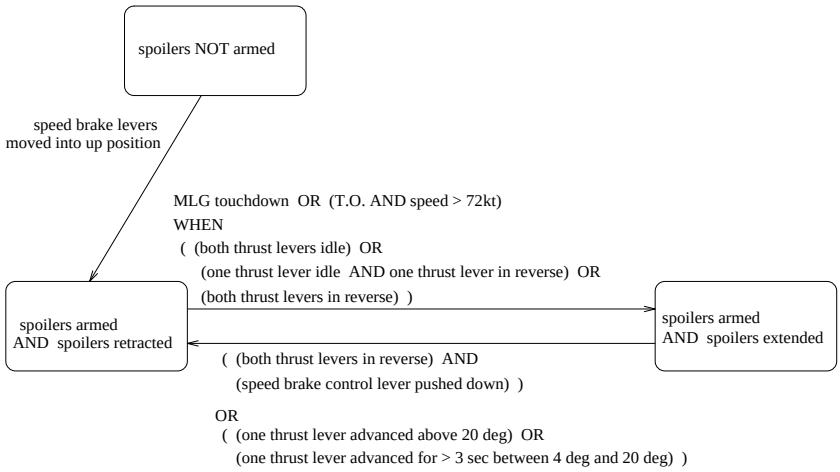

Figure 4: Ground Spoiler Deployment from the FCOM Specification

Using these principles, we have revised the predicate-action diagrams as in Figs 5, 6 and 7.

6 Further Analysis

Some expressions on the FCOM refer to state predicates holding over some explicit period of time. For example, a full logical expression of the description contained in the FCOM must include some logical means of handling assertions of thrust lever position and temporal duration, as noted in [Lad95]. This can be done straightforwardly in TLA [AL94]. In fact, by using TLA, we believe the approach we are suggesting here is extendable to all forms the specification may take, since TLA allows arbitrary mathematics to be included.

When asserting formulas concerning variables which change with time, it's a good idea to list all the potential variables. The list of variables referred to in the FCOM description appears in Table 1. One well-known source of potential inaccuracies is discrepancy between system states which represent certain environmental variables by values derived from sensors, and the actual values of those variables themselves. One example, expressed crudely, is that the Lufthansa A320 suffered delayed deployment of braking systems because, for various reasons expressed in the report [MCAAI94], the sensors didn't detect that the plane was on the runway. See also [FI.93a]. We describe now what must be done with the variables.

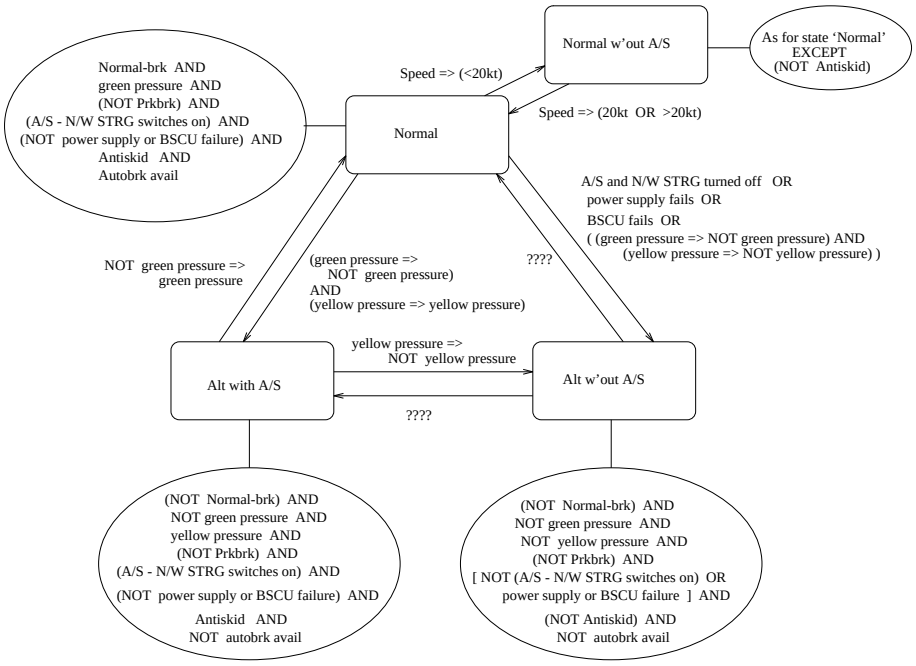

Figure 5: The Revised Braking Modes

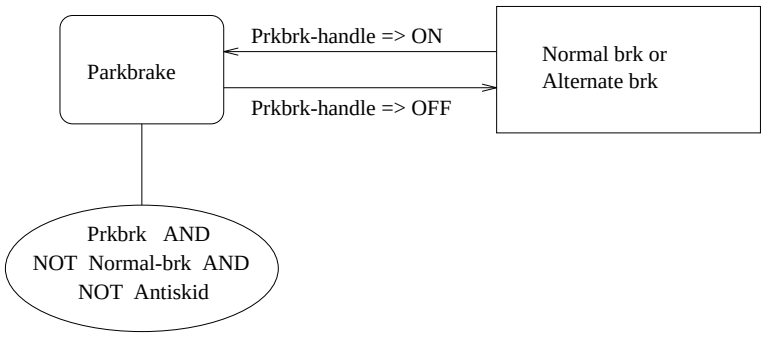

Figure 6: The Revised Parking Brake Mode

Variable name	Values
antiskid-mode	activated, deactivated
autobrake-mode	disarmed, armed, active
braking-on?	Boolean
braking-system-failure?	Boolean
sensed-skid-onset?	Boolean
anti-skid-switch-position	ON, OFF
main-gear-tachometer-left	real-number
main-gear-tachometer-right	real-number
sensed-reference-speed	real-number
brake-release-order-in-effect	Boolean
wheel-slip-value	real-number
green-hydraulic-pressure	available, insufficient
yellow-hydraulic-pressure	available, ??
antiskid-power-electric?	Boolean
autobrake-arming	lo, med, max
speedbrake-control-lever-position	armed, disarmed
sensed-MLG-touch-down?	Boolean
takeoff-run?	Boolean
speed->-72-kt?	Boolean
ground-spoilers-state	armed, extended, in-transit, retracted
thrust-lever-positions	$\{1,2\} \times$ { reverse, idle, $< 4^\circ$, $[4^\circ, 20^\circ]$, $> 20^\circ$ }
number-rudder-pedals-depressed	0,1,2
in-flight?	Boolean
speed-brakes-control-lever-position	up-armed, down-disarmed
sensed-speed	$<$ 20-kts, $[20kts, 72kts]$, $>$ 72-kts
A/SKID	ON, not-ON
N/W-STRG	ON, not-ON
PARKING-BRAKE	ON, not-ON
power-supply-failure?	Boolean
BSCU-failure?	Boolean

Table 1: The variables used in the actuation logic

Variable name	Values
sensed-skid-onset?	Boolean
sensed-reference-speed	real-number
wheel-slip-value	real-number
sensed-MLG-touch-down?	Boolean
takeoff-run?	Boolean
speed->-72-kt?	Boolean
in-flight?	Boolean
sensed-speed	$<$ 20-kts, $[20kts, 72kts]$, $>$ 72-kts

Table 2: Internal variables corresponding to environmental situations

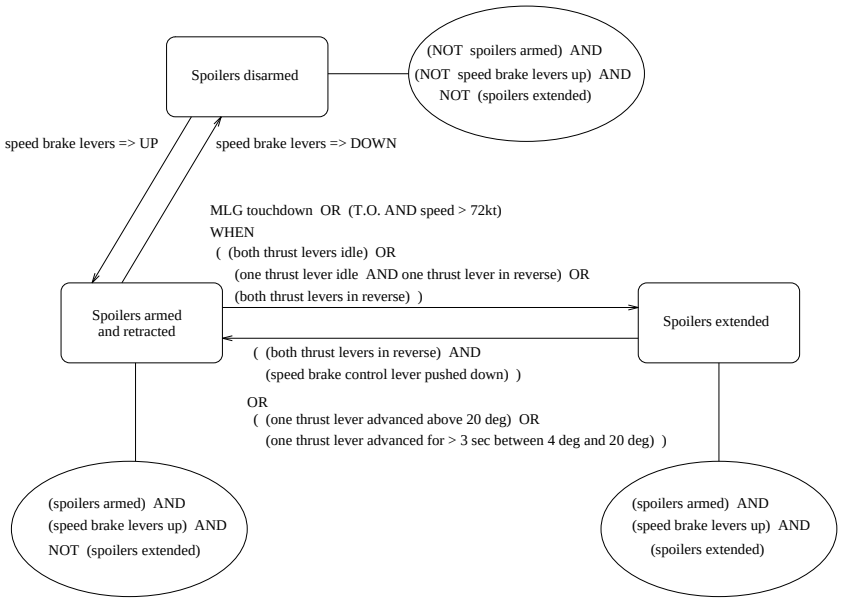

Figure 7: Revised Ground Spoiler Deployment Diagram

Variable name	Values
sensed-skid-onset?	Boolean
sensed-reference-speed	real-number
wheel-slip-value	real-number
sensed-MLG-touch-down?	Boolean
takeoff-run?	Boolean
in-flight?	Boolean

Table 3: Reduced Set of Internal variables corresponding to environmental situations

Listing the Variables

Firstly, all the variables mentioned in the FCOM description should be listed, along with the types of values they can have, which may be determined from the description. These variables determine the possible states, given by their combinations of values. This may be a larger set than needed, because of logical dependencies between some variables. This list may then be surveyed to determine variables which are internal representations of environment variables. Variables which correspond to environmental properties are listed in Table 2 and a reduced set in which variables which are restatements of values of others variables, and thus logically dependent on them, are listed in Table 3.

The three steps involved in analysing the variables are:

- List all variables appearing in the description being considered;
- identify variables which are representations of environmental conditions, and for each such variable *[variable-name]*, add a new variable named *sensed-[variable-name]*;
- identify logical dependencies amongst the variables listed, and reduce the set of variables by elimating those whose values may be expressed as values of others (the choice of which variables to eliminate and which one to retain is arbitrary, subject only to the condition that the eliminated variables may be defined in terms of the retained ones).

7 Conclusions

We have suggested that the description in the Flight Crew Operating Manual of an aircraft such as the A320 may be considered as a high-level system specification of the usual sort. We have shown how predicate-action diagrams, a simple graphical technique based on rigorous logical methods, may be used to analyse the specification, and to express it better.

References

[AL94] M. Abadi and L. Lamport. An old-fashioned recipe for real time. *ACM Transactions on Programming Languages and Systems*, 16(5):1543–1571, Sep 1994.

[Eco94] Air crashes: But surely ... *The Economist*, 331(7866):92–93, June 4th - 10th 1994.

[FB92] J.H. Fielder and D. Birsch. *The DC-10 Case: A Study in Applied Ethics, Technology and Society*. State University of New York Press, 1992.

[FCOM] Airbus Industrie, Toulouse-Blagnac, France. *A320 Flight Crew Operating Manual*. Pages reproduced in [MCAAI94].

[FI.93a] Actuation delay was crucial at Warsaw. *Flight International*, page 10, 13 - 19 October 1993.

[FI.93b] Early Warsaw result provokes questions. *Flight International*, page 14, 3 - 9 November 1993. News report by A. Jeziorski.

[FI.93c] Warsaw over-run was preventable. *Flight International*, page 8, 8 - 14 December 1993.

[Lad95] P. B. Ladkin. Analysis of a technical desciption of the Airbus A320 braking system. *High Integrity Systems*, 1(4), 1995. To appear. Also in `http://www.techfak.uni-bielefeld.de/~ladkin/`.

[Lam94a] L. Lamport. The Temporal Logic of Actions. *ACM Transactions on Programming Languages and Systems*, 16(3):872–923, May 1994.

[Lam94b] L. Lamport. TLA in pictures. In `http://www.research.digital.com/SRC/tla/`, 1994.

[Lev95] N. G. Leveson. *Safeware: System Safety and Computers.* Addison-Wesley, 1995.

[LT82] E. Lloyd and W. Tye. *Systematic Safety.* Civil Aviation Authority, London, 1982.

[MCAAI94] Main Commission Aircraft Accident Investigation. Report on the accident to Airbus A320-211 aircraft in Warsaw on 14 September 1993. Warsaw, March 1994.

[Mel94] P. Mellor. CAD: Computer-Aided Disaster! *High Integrity Systems*, 1(2), November 1994.

[OSZ92] C.V. Oster, J.S. Strong, and C.K Zorn. *Why Airplanes Crash: Aviation Safety in a Changing World.* Oxford University Press, 1992.

[Pot93] J.P. Potocki de Montalk. Computer software in civil aircraft. *Microprocessors and Microsystems*, 17(1):17–23, 1993.

[RTCA92] Radio and Technical Commission for Aeronautics, Washington, D.C. *DO-178B: Software Considerations in Airborne Systems and Equipment Certification*, December 1992. This document is known as EUROCAE ED-12B in Europe.