Chapter 25

The WB-Graph of the 1994 Nagoya Accident

On 26 April 1994, a China Airlines A300 (a non-'fly-by-wire' Airbus) crashed on landing at Nagoya in Japan. It turns out that the pilot flying had inadvertently triggered the 'go-around' mode, as noticed by the captain (the non-flying pilot) but did not disconnect the autopilot, despite repeated instructions from the captain to do so (the A300 Operations Manual explicitly requires the pilot to disconnect the autopilot in such circumstances) until 40 seconds after it was noticed. The pilot flying tried to force the nose of the airplane down, and the autopilot, in go-around mode, reacted to the lack of climb by trimming pitch even further up. When the pilot eventually stopped pushing and the AP was disconnected, the captain took over. However, without the forward pressure on the yoke, the nose rose sharply, due to the extreme nose-up trim, and the plane stalled in an extreme nose-high configuration, and hit the ground tail-first. There were early rumors of unusually high levels of blood alcohol in the pilots' bodies (more than is expected as a natural by-product of death), and a complete power failure before the crash, but neither of these figured in the final report. The question, why the pilot flying did not disconnect the autopilot as he is required to and was instructed to multiple times, probably cannot be answered. As a result of this accident and other recent incidents and accidents, the US FAA started to 'work with' China Air on its pilot training programs.

The final accident report may be found in [Lad]. It is large. We have prepared a textual WB-Graph of the accident from the report. This WB-Graph contains roughly 100 nodes, roughly four times the size of the WB-Graph of the Northwest DC-10 incident, Figure 17.4. We would expect that a full WBA of the Nagoya accident would lead to an increase in the number of nodes in the WB-Graph, but we judge it unlikely that it would lead to, say, a ten-fold increase. a ten-fold increase in the number of nodes would make the Nagoya WB-Graph roughly forty times the size of the graph in Figure 17.4. Since the number of causal-factor edges in a WB-Graph appears to be roughly linear in the number of nodes (see

Figures 23.5 and 24.1 as well as Figure 17.4), we conclude that a complete WBA proof for the Nagoya accident would use less than (we expect in fact considerably less than) forty times the effort required for the proof in Chapter 22 of the WBA for the example whose WB-Graph is Figure 17.4. Such an effort we judge to be feasible for an accident investigation, given technical expertise with hierarchical proofs in EL.

We include the Nagoya textual WB-Graph here as the basis for our comments, above, on complexity.

```
[0] /* AC crashes into landing zone near E1 taxiway
// @T11:15’45" */
  /\{1} /* AC stalls since
   // @T11:15’31" */
  /\{2} /* CRW unable to recover stall */

  {1} {-.1} /* AOA becomes too large */

    {1.1} /\<-.1> /* AC in out of trim (nose high) condition */
  /\<-.2> /* AC climbing steeply */
          /\{-.3} /* CAS becomes too low */

      <1.1.1> /\<-.1> /* THS at -12.3 degrees (=nose-up) since: [1.1.1.1.1] */
              /\<-.2> /* Elevators in nose-down position */
              /\(-.3) /* CRW does not correct out of trim condition */

        <1.1.1.1> /\<-.1> /* AP is engaged in CMD
// @T11:14’18" */
                  /\<-.2> /* AP in GA mode */
  /\{-.3} /* F/O pushing on control column */
  /\{-.4} /* AP stays engaged, although {1.1.1.1.3} */
          /\{-.5} /* CRWs hand-tuning attempts ineffective
// #ACTION# // @T11:14’20" // @T11:14’34" // @T11:14’39" */

          <1.1.1.1.1> [-.1] /* AP engaged
    // #ACTION# // @T11:14’18" */
          <1.1.1.1.2> /\[-.1] /* F/O (PF) triggers GA-lever
    // @T11:14’05" // inf CVR */
                      /\(-.2) /* F/O (PF) does not disengage GA mode although
advised to do so by CAP several times:
    // @T11:14’10" // @T11:14’30" // @T11:14’45" */

            [1.1.1.1.2.1] /\<-.1> /* position of GA-lever
    // ASSUMPTION */
  /\[-.2] /* F/O moves hand on throttles
    // ASSUMPTION */

      <1.1.1.1.2.1.1> <-.1> /* Airbus Industry Cockpit Layout */
```

Figure 25.1: The Nagoya WB-Graph, Part 1

```
          (1.1.1.1.2.2) /\{-.1} /* F/O (PF) tries but does not succeed in
    disengaging GO-AROUND-mode
  // #ACTION# */
  /\<-.2> /* F/O (PF) does not realize his actions didn't
    succeed
  // #PERCEPTION# */

            {1.1.1.1.2.2.1} /\[-.1] /* F/O (PF) tries to go direct into LAND mode
  // #INTENTION# // inf CVR */
      /\<-.2> /* direct access to LAND mode button cannot
        disengage GO AROUND mode */

<1.1.1.1.2.2.1.1> <1.1.1.1.5.3.1>

                <1.1.1.1.2.2.1.2> <1.1.1.1.4.1>

              <1.1.1.1.2.2.2> /\<-.1> /* F/O (PF) overextended with situation
// ASSUMPTION */
      /\<-.2> /* high workload
// #ATTENTION# */

  <1.1.1.1.4> /\<-.1> /* Airbus Industry AP logic */
      /\(-.2) /* modification to AP prescribed in Service Bulletin
      SB A300-22-6021 had not been incorporated into
      the aircraft
// 3rd party Information */

    (1.1.1.1.4.2) /\(-.1) /* The aircraft manufacturer did not categorise
     the SB A300-22-6021 as "Mandatory"
// 3rd party Information */
  /\(-.2) /* The airworthiness authority of the nation of
     design and manufacture did not issue promptly
     an airworthiness directive pertaining to
     implementation of the SB.
// 3rd party Information */
```

Figure 25.2: The Nagoya WB-Graph, Part 2

```
  {1.1.1.1.3} /\{-.1} /* F/O (PF) tries to recover optimal glide path */
      /\<-.2> /* F/O (PF) believes nose-down elevator commands will
        achieve nose-down state
// ASSUMPTION */

    {1.1.1.1.3.1} /\{-.1} /* AC left optimal glide path */
  /\<-.2> /* AC should return to optimal glide path */

              {1.1.1.1.3.1.1} [1.1.1.1.2.1]
// inf CVR */

    <1.1.1.1.3.2> <1.1.1.1.5.3.1>

  {1.1.1.1.5} /\[-.1] /* CRW attempts to hand-tune */
      /\<-.2> /* when active, AP doesn't allow THS override */
      /\(-.3) /* CRW doesn't realize <1.1.1.1.5.2>
// #PERCEPTION# */
      /\<-.4> /* CRW lacks experience and knowledge with A300 AP
// ASSUMPTION */

    [1.1.1.1.5.1] {1.1.1.1.3.1}

    <1.1.1.1.5.2> <1.1.1.1.4.1>

    (1.1.1.1.5.3) <1.1.1.1.5.4>

        <1.1.1.2> {1.1.1.1.3}
```

Figure 25.3: The Nagoya WB-Graph, Part 3

```
        (1.1.1.3) (-.1) /* CRW does not recognize OOT condition
// #PERCEPTION# // inf CVR */


  (1.1.1.3.1) /\<-.1> /* optical systems for the purpose of THS motion
      awareness do not provide effective information
      at night */
             /\<-.2> /* optical/acoustical warning device, capable of
      _actively_ alerting THS motion inactive */
                     /\<-.3> /* CRW does not pay attention
// #ATTENTION# // inf CVR */

            <1.1.1.3.1.1> <1.1.1.1.2.1.1.1>

    <1.1.1.3.1.2> /\[-.1] /* Airbus Industry eliminated function from AP
  in CMD mode design
  // 3rd party information */
  /\<-.2> /* Airbus Industry did not establish another
  warning and recognition function
  // 3rd party information */
  /\<1.1.1.1.1>

      <1.1.1.3.1.2.1> {-.1} /* Airbus Industry followed suggestion from UK CAA */
```

Figure 25.4: The Nagoya WB-Graph, Part 4

```
      <1.1.2> /\<-.1> /* high engine thrust */
              /\<-.2> /* F/O releases control wheel */
      /\<1.1.1>
      /\<1.1.1.1>

        <1.1.2.1> [-.1] /* EPR increased from 1.04 to > 1.6 */

          [1.1.2.1.1] /\[-.1] /* THR levers moved forward
// @T11:15'11" */
      /\[-.2] /* Alpha Floor Function activated
// @T11:14'57" // @H570 */

            [1.1.2.1.1.1] [-.1] /* CAP(PF) decides to initiate GO-AROUND manouevre
// @T11:15'03" */

    <1.1.2.1.1.2> /\<-.1> /* AOA exceeded threshold AOA of 11.5 degrees */
  /\<-.2> /* pitch angle increased */
  /\<-.3> /* AP disengaged
// @T11:14'50" */
  /\<-.4> /* Airbus Industry Logic */

      <1.1.2.1.1.2.1> /\<1.1.1>
      /\{1.1.3}

              <1.1.2.1.1.2.2> /\<1.1.1>
      /\<1.1.2.1>
// causal feedback loop !! - alpha floor //
```

Figure 25.5: The Nagoya WB-Graph, Part 5

```
      {1.1.3} /\<-.1> /* THR not engaged continuously */
              /\{-.2} /* THR decreased temporarily */
      /\<1.1.2>

        <1.1.3.1> /\<-.1> /* CAP(PF) uncertain about situation
// #ATTENTION# */
                  /\[-.2] /* CRWs actions interfere with AP operation */

  <1.1.3.1.2> /\[-.1] /* F/O (PF) interrupts execution of Alpha Floor function */
      /\<-.2> /* A300 AP 'intended to permit pilots to apply
      _small_ manual control inputs to assist the AP'
// cite from FCOM */
                      /\<-.3> /* CRW unaware that A300 AP does not allow
      permanent manual override
// #ATTENTION# */

    [1.1.3.1.2.1] {-.1} /* F/O (PF) counteracts against resulting pitch-up
movement from [1.1.2.1.1.2] */

      <1.1.3.1.2.1.1> <-.1> /* F/O (PF) doesn't realize [1.1.2.1.1.2]
// #ATTENTION# */

            <1.1.3.1.2.2> <1.1.1.1.4.1>

    <1.1.3.1.2.3> /\<-.1> /* CRW unable to gain this information
  from FCOM */
  /\<-.2> /* CAP's (PF) action would be appropriate
  for Boeing AP
  // ASSUMPTION */
  /\<1.1.1.1.5.3.1>

              <1.1.3.1.2.3.1> <-.1> /* FCOM design not suited for handling
    alert situations
    // ASSUMPTION */

<1.1.3.1.2.3.1.1> <-.1> /* Airbus Industry FCOM layout */

        {1.1.3.2} /\[-.1] /* THR levers retarded temporarily */
                  /\<-.2> /* surges occurred in both engines */

  [1.1.3.2.1] /\[-.1] /* CAP (PNF) intends to continue approach
// inf CVR */
      /\<1.1.3.1.2.1>

  <1.1.3.2.2> <-.1> /* high AOA of inlets */

    <1.1.3.2.2.1> /\<1.1.2>
  /\{1.1.3}
```

Figure 25.6: The Nagoya WB-Graph, Part 6

```
 {2} /\(-.1) /* CRW doesn’t take appropriate action to recover stall */
   /\<-.2> /* AC systems in unusual modes */
   /\<-.3> /* time and altitude for recovery operations short to insufficient */

  (2.1) /\<-.1> /* CRW not aware of AC systems states
 // #ATTENTION# */

   <2.1.1> /\<-.1> /* situation is unusual */
   /\<-.2> /* no THS motion warning */
   /\<-.3> /* none of the CRW is able to keep track of the
   situation
   // #ATTENTION# */
   /\<1.1.3.1.2.1.1.1>

<2.1.1.1> /\<-.1> /* transition ‘GO-AROUND -> LAND’ is no flight manoevre
 according to Standard Operating Procedures */

<2.1.1.2> /\<1.1.1.3.1.1>
 /\<1.1.1.3.1.2>

<2.1.1.3> /\[-.1] /* CAP (PNF) takes over controls against duty assignment
 // #ACTION# // @T11:15’03" */
 /\<-.2> /* CAP (PNF) doesn’t grasp flight conditions
 // inf CVR */
 /\{-.3} /* F/O (PF) looses his autonomy, since he follows a series of
 instructions given by CAP (PNF) instead of acting on his own
 // @T11:14’26" to T11:15’03" */

  <2.2> <-.1> /* complex control situation at stall */

   <2.2.1> /\<-.1> /* trying to transit GO-AROUND -> LAND */
   /\<1.1.2.1.1.2>
   /\<1.1.1>

  <2.3> /\<-.1> /* nose-up attitude is 43.8 degrees */
 /\<-.2> /* altitude is 1,730ft */
     /\<-.3> /* AS is less than 50kts */


(88 nodes)
```

Figure 25.7: The Nagoya WB-Graph, Part 7

```
Semantics:
===========
[X.X]   Event
<Y.Y>   State
{Z.Z}   Process
(U.U)   Non-Event

/* comment on node */

additional information on comments:

// @T...  T=Time (hh:mm'ss" UTC)
// @H...  Predicates: H=Heigh (pressure altitude in ft)
// @P...  P=Position (2D)

// #<classification_of_failure>#  where
    <classification_of_failure> ::= perception | attention | reasoning |
                                    decision | intention | action
   is the classification of failures according to the extended
   information-processing model introduced in [GLL96]

// 3rd party information
// inf CVR   any information judged as required
// ...
```

Figure 25.8: Notational Key for the Nagoya WB-Graph

GLOSSARY:
=========

AD	: Airworthiness Directive
ADC	: Air Data Computer
AFS	: Automatic Flight System
ALT	: Altitude
ALT SEL	: Altitude Selector
AOA	: Angle of Attack
AP	: Auto-Pilot
APU	: Auxiliary Power Unit
A/THR	: Automatic Thrust
AT	: Auto Throttle
ATS	: Auto-Throttle System
ATT	: Attitude
BEA	: Bureau Enqu^etes Accidents
BKN	: Broken
CAP	: Captain
CAS	: Computed Airspeed
CGCC	: Center of Gravity Control Computer
CAT	: Category
CMD	: Command
CN	: Consigne de Navigabilite
CRW	: Crew
CVR	: Cockpit Voice Recorder
CWS	: Control Wheel Steering
DFDR	: Digital Flight Data Recorder
DGAC	: Direction G^en^erale de l’ Aviation Civile
ECAM	: Electronic Centralized Aircraft Monitoring
BFCU	: Electronic Flight Control Unit
EFIS	: Electronic Flight Instrument System
ENG	: Engine
EPR	: Engine Pressure Ratio
FAA	: Federal Aviation Administration
FAC	: Flight Augmentation Computer
FADEC	: Full Authority Digital Electronic Control
FCC	: Flight Control Computer
FCOM	: Flight Crew Operating Manual
FCU	: Flight Control Unit
FD	: Flight Director
FIDC	: Fault Isolation and Detection Computer
FIDS	: Fault Isolation and Detection System
FL	: Flight Level
FMA	: Flight Mode Annunciator
FMC	: Flight Management Computer
FMS	: Flight Management System
F/O	: First Officer
FMC	: Flight Warning Computer

Figure 25.9: Glossary for the Nagoya WB-Graph, Part 1

GA	: GO AROUND
GCU	: Generator Control Unit
GPWC	: Ground Proximity Warning Computer
GPWS	: Ground Proximity Warning System
GS	: Glide Slope
HDG	: Heading
HDG/SEL	: Heading Selector
HPC	: High Pressure Compressor
HPT	: High Pressure Turbine
ICAO	: International Civil Aviation Organization
IGS	: Instrument Guidance System
IGV	: Inlet Guide Vane
IND	: Indicator
ILS	: Instrument Landing System
IRS	: Inertial Reference System
IRU	: Inertial Reference Unit
LAND	: Landing
L/D	: Landing
LIG	: Landing Gear
LOC	: Localizer
LPC	: Low Pressure Compressor
LPT	: Low Pressure Turbine
LVL/CH	: Level Change
MAC	: Mean Aerodynamic Chord
MAN THR	: Manual Thrust
MIC	: Microphone
MTP	: Maintenance and Test Panel
NAV	: Navigation
NTSB	: National Transportation Safety Board
OOT	: Out Of Trim
OVC	: Overcast
PCM	: Pulse Code Modulation
PF	: Pilot Flying
PFD	: Primary Flight Display
PlC	: Pilot in Command
PNF	: Pilot Not Flying
QNH	: Pressure Setting to Indicate Elevation above Mean Sea Level

Figure 25.10: Glossary for the Nagoya WB-Graph, Part 2

R ALT	: Radio Altitude
RET	: Retract
RMI	: Radio Magnetic Indicator
RWY	: Runway
SB	: Service Bulletin
SCT	: Scattered
SGU	: Symbol Generator Unit
SPD	: Speed
SPD/MAC	: Speed/Mach
SRS	: Speed Reference System
SW	: Switch
TCC	: Thrust Control Computer
TCD	: Ministry of Transport Civil Aviation Bureau Directive
THR	: Thrust
THR L	: Thrust Latch
THS	: Trimmable Horizontal Stabilizer
TIPS	: Technical Instruction Processing Sheet
TRP	: Thrust Rating Panel
VAPP	: Approach Target Speed
VOR	: VHF Omnidirectional Radio Range
V/S	: Vertical Speed
Vs	: Stall Speed
VTG	: Target Speed
W.STA	: Wing Station

Figure 25.11: Glossary for the Nagoya WB-Graph, Part 3

Bibliography

[Ada95] John Adams. *Risk.* UCL Press, London, 1995.

[Aer96] Aeronautica Civil of The Republic of Colombia. *Aircraft Accident Report: Controlled Flight Into Terrain, American Airlines Flight 965, Boeing 757-223, N651AA, Near Cali, Colombia, December 20, 1995.* Author, Santafe de Bogota, D.C.-Colombia, Sep 1996. Also available at [LR].

[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.

[And58] A. R. Anderson. A reduction of deontic logic to alethic modal logic. *Mind*, 67:100–103, 1958.

[AS85] Bowen Alpern and Fred B. Schneider. Defining liveness. *Information Processing Letters*, 21:181–185, 1985.

[Ato76] Atomic Industrial Forum. Committee on reactor licensing and safety statement on licensing reform. Technical report, Author, New York, 1976.

[Aus75] J. L. Austin. *How To Do Things With Words.* Oxford University Press, Oxford, 2nd edition, 1975.

[Aut00] U.K. Civil Aviation Authority. Interference levels in aircraft at radio frequencies used by portable telephones. Technical Report 9/40-23-90-02, Author, May 2000. Available from `http://www.srg.caa.co.uk/srg/srg_news.asp`.

[Bec86] Ulrich Beck. *Risikogesellschaft: Auf dem Weg in eine andere Moderne.* Suhrkamp Verlag, Frankfurt am Main, 1986.

[Blu97] Michael Blume. Kleine Einführung in die Spezifikationssprache TLA+. Technical Report RVS-LN-06, RVS Group, Faculty of Technology, University of Bielefeld, 1997. Tutorial.

[Boa95] U.S. National Transportation Safety Board. Factual data [in the cali accident]. Available from [Lad], Dec 1995.

[Boa96] US National Transportation Safety Board. Safety recommendation (including a-96-90 through a-96-106). Also available at [LR], Oct 1996.

[CL79] B. Cohen and I. S. Lee. A catalog of risks. *Health Physics*, 36:707–722, 1979.

[Dah86] Roald Dahl. *Boy.* Penguin Books, London, 1986.

[Dak91] Karl Dake. Orienting dispositions in the perception of risk: an analysis of contemporary worldviews and cultural biases. *Journal of Cross-Cultural Psychology*, 22(1):61–82, 1991.

[Dak92] Karl Dake. Myths of nature: Culture and the social construction of risk. *Journal of Social Issues*, 48:21–37, 1992.

[Dav80] Donald Davidson. *Essays on Actions and Events.* Oxford University Press, Oxford, 1980.

[Deg96] Asaf Degani. *Modelling Human-Machine Systems: On Modes, Error, and Patterns of Interaction.* PhD thesis, Georgia Institute of Technology, December 1996. Available from the author at NASA Ames Research Center.

[DW82] Mary Douglas and Aaron Wildavsky. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers.* University of California Press, Berkeley, Los Angeles and London, 1982.

[dWL95] H. de Wulf and D. Learmount. DC-10 misses Frankfurt runway – by 300km. *FLIGHT INTERNATIONAL*, 148(4493):8, 11-17 October 1995.

[FB92] John H. Fielder and Douglas Birsch, editors. *The DC-10 Case.* State University of New York Press, Albany, New York, 1992.

[Fel90] Fellowship of Engineering. Warnings of preventable disasters conference. Author, London, 6 September 1990.

[Fis00] Franklin A. Fisher. Some Notes on Sparks and Ignition of Fuels. Technical Report NASA/TM-2000-210077, NASA/Lightning Technologies Inc., Langley Research Center, Hampton, VA, March 2000.

[FLSDK81] Baruch Fischhoff, Sarah Lichtenstein, Paul Slovic, Stephen L. Derby, and Ralph L. Keeney. *Acceptable Risk.* Cambridge University Press, Cambridge, U.K., 1981.

[Gar98] Ken E. Garlington. Personal communication. June 1998.

[Ger97] T. Gerdsmeier. A tool for building and analysing WB-Graphs. Technical Report RVS-RR-97-02, RVS Group, Faculty of Technology, University of Bielefeld, Feb 1997. Available at [LR].

[Gib] Dafydd Gibbon. The parable of next thursday. Available from `http://coral.lili.uni-bielefeld.de/~gibbon`.

[GL96] D. Gibbon and P. B. Ladkin. Comments on Confusing Conversation at Cali. Technical Report RVS-RR-96-10, RVS Group, Faculty of Technology, University of Bielefeld, Feb 1996. Available at [LR].

[GLL97a] T. Gerdsmeier, P. Ladkin, and K. Loer. Analysing the Cali accident with a WB-Graph. In *Proceedings of the first Workshop on Human Error and Systems Development, Glasgow, Scotland*, volume TR-97-2, pages 2–15, March 1997. Also available as RVS-RR-97-02 in [LR].

[GLL97b] T. Gerdsmeier, P. Ladkin, and K. Loer. Formalising Failure Analysis. Technical Report RVS-Occ-97-06, Networks and distributed Systems Group, Faculty of Technology, Bielefeld University, Bielefeld, Germany, 1997. Available from [LR].

[GNRR93] R. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors. *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*. Springer-Verlag, 1993.

[Gro96] Boeing Commercial Airplane Group. Statistical Summary of Commercial Jet Aircraft Accidents, Worldwide Operations, 1959-1995. Technical report, Author, Seattle, Washington, 1996. Produced annually.

[Haa78] Susan Haack. *Philosophy of Logics.* Cambridge University Press, Cambridge, 1978.

[Haa96] Susan Haack. *Deviant Logic, Fuzzy Logic.* University of Chicago Press, Chicago, 1996.

[HC96] G.E. Hughes and M. Creswell. *A New Introduction to Modal Logic.* Routledge, London, 1996.

[HE97] U.K. Health and Safety Executive. Dispensing petrol as a fuel- health and safety guidance for employees. Document C338 IND(G)216L, 2/97, available at `http://www.hse.gov.uk/pubns/indg216.htm`, 1997.

[Hil93] Mayer Hillman. *Cycle Helmets: the case for and against.* Policy Studies Institute, London, 1993.

[HL97] M. Höhl and P. Ladkin. Analysing the 1993 Warsaw accident with a WB-Graph. Technical Report RVS-Occ-97-09, Networks and distributed Systems Group, Faculty of Technology, Bielefeld University, Bielefeld, Germany, 1997. Available through [LR].

[HL98] Michael Höhl and Peter B. Ladkin. Analysing the 1993 Warsaw Accident with a WB-Graph. Technical Report RVS-Occ-97-09, Networks and distributed Systems Group, Faculty of Technology, Bielefeld University, Bielefeld, Germany, 1998.

[Höh98] Michael Höhl. *wb2dot.* Software RVS-Soft-04, RVS Group, Faculty of Technology, University of Bielefeld. Available through http://www.rvs.uni-bielefeld.de, Mar 1998.

[Hol79] C. S. Holling. Myths of ecological stability. In G. Smart and W. Stanbury, editors, *Studies in Crisis Management.* Butterworth, Montreal, 1979.

[Hol86] C. S. Holling. The resilience of terrestrial ecosystems. In W. Clark and R. Munn, editors, *Sustainable development of the biosphere.* Cambridge University Press, Cambridge, U.K., 1986.

[Hor97] Jennifer Hornsby. *Simple Mindedness: In Defence of Naive Naturalism in the Philosophy of Mind.* Harvard University Press, Cambridge, MA, 1997.

[Hum75] David Hume. *An Enquiry Concerning Human Understanding.* Oxford University Press, third edition, 1777/1975. Ed. L. A. Selby-Bigge and P. H. Nidditch.

[HV76] M. Hynes and E. Vanmarcke. Reliability of embankment performance predictions. In *Proceedings of the ASME Engineering Mechanics Division Speciality Conference*, Waterloo, Canada, 1976. ASME, University of Waterloo Press.

[Jer97] Robert Jervis. *System Effects: Complexity in Political and Social Life.* Princeton University Press, New Jersey, 1997.

[Joh97] C. W. Johnson. The epistemics of accidents. *International Journal of Human-Computer Studies*, 47:659–688, 1997.

[KH99] Daniel M. Kammen and David M. Hassenzahl. *Should We Risk It?: Exploring Environmental, Health, and Technological Problem Solving.* Princeton University Press, Princeton, N.J., 1999.

[KKS93] Paul R. Kleindorfer, Howard C. Kunreuther, and Paul J. H. Shoemaker. *Decision Sciences: An Integration Perspective.* Cambridge University Press, Cambridge, U.K., 1993.

[KLST71] David H. Krantz, R. Duncan Luce, Patrick Suppes, and Amos Tversky. *Foundations of Measurement, Volume 1: Additive and Polynomial Representations.* Academic Press, New York, London, 1971.

[KST82] Daniel Kahneman, Paul Slovic, and Amos Tversky, editors. *Judegement under uncertainty: Heuristics and biases.* Cambridge University Press, Cambridge, U.K., 1982.

[Lad] Peter B. Ladkin et al. Computer-related incidents with commercial aircraft. Technical Report RVS-Comp-01, RVS Group, Faculty of Technology, University of Bielefeld. Compendium of digitised accident reports and commentary, available through [LR].

[Lad95a] P. Ladkin. Fly NorthWest Airlines to unknown destinations. *The Risk Digest*, 17(38), October 1995. `http://catless.ncl.ac.uk/Risks/17.38.html#subj1`.

[Lad95b] P. Ladkin. Re: Fly NorthWest Airlines to unknown destinations. *The Risk Digest*, 17(40), October 1995. `http://catless.ncl.ac.uk/Risks/17.40.html#subj3`.

[Lad96a] Peter Ladkin. Explaining Failure with Tense Logic. Technical Report RVS-RR-96-13, Networks and distributed Systems Group, Faculty of Technology, Bielefeld University, Bielefeld, Germany, 1996. Available through [LR].

[Lad96b] Peter Ladkin. Some Dubious Theses in the Tense Logic of Accidents. Technical Report RVS-RR-96-14, Networks and distributed Systems Group, Faculty of Technology, Bielefeld University, Bielefeld, Germany, 1996. Available through [LR].

[Lad97] Peter Ladkin. Using the Temporal Logic of Actions: A Tutorial on TLA Verification. Technical Report RVS-RR-97-08, Networks and distributed Systems Group, Faculty of Technology, Bielefeld University, Bielefeld, Germany, 1997. Invited Tutorial on TLA, Second International Conference on Temporal Logic, Manchester, England, 14-18 July, 1997, also available through [LR].

[Lad99] Peter B. Ladkin. On classification of factors in failures and accidents. Technical Report RVS-Occ-99-04, RVS Group, Faculty of Technology, University of Bielefeld, July 1999. Available through [LR].

[Lam] Leslie Lamport. The Temporal Logic of Actions (TLA) Page. `http://www.research.digital.com/ tla/`.

[Lam86] Leslie Lamport. The mutual exclusion problem: Part I – A theory of interprocess communication. *Journal of the ACM*, 33:313–326, April 1986.

[Lam93a] Leslie Lamport. How to Write a Proof. Available through [Lam], February 1993.

[Lam93b] Leslie Lamport. Hybrid systems in TLA$^+$. In *[GNRR93]*, pages 77–102, 1993.

[Lam94a] Leslie Lamport. How to write a long formula. *Formal Aspects of Computing*, 6:580–584, 1994.

[Lam94b] Leslie Lamport. The temporal logic of actions. *ACM Transactions on Programming Languages and Systems*, 16(3):872–923, May 1994.

[Lam94c] Leslie Lamport. The temporal logic of actions. *ACM Transactions on Programming Languages and Systems*, 16(3):872–923, May 1994. Also available through [Lam].

[Lam95a] L. Lamport. TLA in pictures. In *IEEE Transactions in Software Engineering 21(9)*, pages 768–775, 1995. Also available through [Lam].

[Lam95b] Leslie Lamport. How to write a proof. *American Mathematical Monthly*, 102(7):600–608, August-September 1995. Also available as [Lam93a].

[Lam96] Leslie Lamport. The Module Structure of TLA+. September 1996. SRC Technical Note 1997-002, available from `research.compaq.com/SRC/publications/`.

[Lam97] Leslie Lamport. The Operators of TLA+. April 1997. SRC Technical Note 1997-006a, available from `research.compaq.com/SRC/publications/`.

[Lap92] J.-C. Laprie, editor. *Dependability: Basic Concepts and Terminology, in English, French, German, Italian and Japanese*, volume 5 of *Dependable Computing and Fault Tolerance.* Springer-Verlag, Wien, New York, 1992. Prepared by IFIP Working Group 10.4 on *Dependable Computing and Fault Tolerance.*

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

[Lev00] Nancy G. Leveson. Personal communication. February 2000.

[Lew73a] David Lewis. Causation. *Journal of Philosophy*, 70:556–567, 1973. Also in [Lew86, ST93].

[Lew73b] David Lewis. *Counterfactuals*. Oxford University Press, Inc., Blackwell, 1973.

[Lew86] David Lewis. *Philosophical papers, Vol.II.* Oxford University Press, Inc., 200 Maddison Avenue, New York, New York 10016, 1986.

[Lew90] H. W. Lewis. *Technological Risk*. Norton, New York and London, 1990.

[Lip91] Peter Lipton. *Inference to the Best Explanation*. Routledge, 1991.

[LL32] C.I. Lewis and C.H. Langford. *Symbolic Logic*. Dover Publications, New York, 1932.

[LL98] Peter Ladkin and Karsten Loer. Analysing Aviation Accidents using WB-Analysis – An Application for Multimodal Reasoning. to appear in *AAAI Spring Symposium on Multimodal Reasoning*, Stanford, California, March 1998.

[LP96] Peter Ladkin and Everett Palmer. An Analysis of 'Oops'. Unpublished preprint, November 1996.

[LR] Peter Ladkin and RVS Group. RVS Group Publications. RVS Group, Technische Fakultät, Universität Bielefeld. Available through `http://www.rvs.uni-bielefeld.de`.

[LT82] E. Lloyd and W. Tye. *Systematic Safety: Safety Assessment of Aircraft Systems*. Civil Aviation Authority, London, 1982.

[Luh91] Niklas Luhmann. *Soziologie des Risikos*. Walter de Gruyter, Berlin, New York, 1991.

[Mac74] J. L. Mackie. *The Cement of the Universe: A Study of Causation*. Clarendon Press, Oxford, 1974.

[Mar92] A. Marin. Costs and benefits of risk reduction. Appendix to [Roy92], 1992.

[Mel97] Alfred R. Mele, editor. *The Philosophy of Action*. Oxford Readings in Philosophy. Oxford University Press, Oxford, 1997.

[Mel00] Peter Mellor. Personal communication. February 2000.

[MH90] M. Granger Morgan and Max Henrion. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis.* Cambridge University Press, Cambridge, U.K., 1990.

[MHCM96] J. Moffett, J. Hall, A. Coombes, and J. McDermid. A Model for a Causal Logic for Requirements Engineering. *Journal of Requirements Engineering*, 1(1):27–46,, March 1996.

[Mil73a] John Stuart Mill. *A System of Logic, Books I-III*, volume VII of *Collected Works.* University of Toronto Press, London: Routledge & Kegan Paul, 1973.

[Mil73b] John Stuart Mill. *Collected Works Vol. VIII – A System of Logic, Books IV-VI.* University of Toronto Press, London: Routledge & Kegan Paul, 1973.

[Min89] Ministry of Planning, Housing, Transport and Maritime Affairs (France). Investigation Commission concerning the accidents which occurred on June 26th 1988 at Mulhouse-Habsheim (68) to the Airbus A320, registered F-GFKC. Final Report, November 29th 1989.

[MLO98] Claire Marris, Ian H. Langford, and Timothey O'Riordan. A quantitative test of the cultural theory of risk perceptions: Comparison with the psychometric paradigm. *Risk Analysis*, 18(5):635–647, October 1998.

[MWD78] J.J.-Ch. Meyer, R.J. Wieringa, and F.P.M. Dignum. The Role of Deontic Logic in the Specification of Information Systems. In Jan Chomicki and Gunter Saake, editors, *Logics for Databases and Information Systems.* Kluwer Academic Publishers, 1997/8.

[NAS] NASA. Human Factors -Mission Statement. Office of Aeronautics homepage, `http://olias.arc.nasa.gov/mission.html`.

[Nat96] National Research Council Committee on Risk Characterization. *Understanding Risk.* National Academy Press, Washington, D.C., 1996.

[Nol94] Michael S. Nolan. *Fundamentals of Air Traffic Control.* Wadsworth Publishing Company, Belmont, California 94002, 1994.

[Nor] Stephen North et al. *graphviz* – tools for viewing and interacting with graph diagrams. Available through http://www.research.att.com/sw/tools/graphviz/.

[NS75] R. Näätänen and H. Summala. *Road-user behavior and traffic accidents.* North-Holland, Amsterdam, 1975.

[Pal95] Everett Palmer. Oops, it didn't arm. – A Case Study of Two Automation Surprises. In *Proceedings of the 8th International Symposium on Aviation Psychology*, 1995. Also available through http://olias.arc.nasa.gov.

[Per84] Charles Perrow. *Normal Accidents: Living with High-Risk Technologies.* New York: Basic Books, 1984.

[Pet85] Henry Petrowski. *To Engineer is Human: The Role of Failure in Successful Design.* St. Martin's Press, 1985. Paperback edition, Vintage Books, 1992.

[Pet94] Henry Petrowski. *Design Paradigms: Case Histories of Error and Judgement in Engineering.* Cambridge University Press, 1994.

[PL97] E. A. Palmer and P. B. Ladkin. Analysing an 'oops' incident. Unpublished manuscript, 1997.

[Pra65] Dag Prawitz. *Natural Deduction: A Proof-Theoretical Study.* Almqvist and Wiksell, Uppsala, 1965.

[Qui64] Willard Van Orman Quine. *From a Logical Point of View.* Harvard University Press, second edition, 1964. Revised.

[Rap81] E. Rappoport. *Unpublished doctoral dissertation.* PhD thesis, University of California, Los Angeles, 1981.

[Res87] Michael D. Resnick. *Choices: An Introduction to Decision Theory.* University of Minnesota Press, Minneapolis, 1987.

[Roy83] Royal Society. *Risk assessment: a study group report.* Author, London, 1983.

[Roy92] Royal Society. *Risk: analysis, perception and management.* Author, London, 1992.

[Rv93] John Rushby and Friedrich von Henke. Formal verification of algorithms for critical systems. *IEEE Transactions on Software Engineering*, 19(1):13–23, Jan 1993.

[Sag93] Scott D. Sagan. *The Limits of Safety: Organisations, Accidents and Nuclear Weapons.* Princeton University Press, New Jersey, 1993.

[Sea69] John R. Searle. *Speech Acts.* Cambridge University Press, Cambridge, 1969.

[Sea83] John R. Searle, editor. *Intentionality.* Cambridge University Press, Cambridge, 1983.

[SF85] Kirstin Shrader-Frechette. *Risk Analysis and Scientific Method.* D. Reidel Publishing Company, Dordrecht, Netherlands, 1985.

[SF91] Kirstin Shrader-Frechette. *Risk and Rationality.* University of California Press, Berkeley and Los Angeles, CA, 1991.

[SFL82] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein. Facts versus fears: Understanding perceived risk. In Daniel Kahneman, Paul Slovic, and Amos Tversky, editors, *Judgement Under uncertainty: Heuristics and biases.* Cambridge University Press, Cambridge, U.K., 1982.

[Sky99] Brian Skyrms. *Choice and Chance: An Introduction to Inductive Logic.* International Thompson Publishing, fourth edition, 1999.

[SM95] Mandayam K. Srivas and Stephen P. Miller. Formal verification of an avionics microprocessor. Technical Report SRI-CSL-95-4, SRI International, Computer Science Laboratory, Menlo Park, California, 1995. Available at `http://www.csl.sri.com/csl-95-4.html`.

[ST90] M. Schwarz and M. Thompson. *Divided We Stand: Redefining politics, technology and social choice.* Harvester Wheatsheaf, Hemel Hempstead, 1990.

[ST93] Ernest Sosa and Michael Tooley, editors. *Causation.* Oxford Readings in Philosophy. Oxford University Press, Oxford, 1993.

[ST95] Eldar Shafir and Amos Tversky. Decision making. In Daniel N. Osherson, editor, *An Invitation to Cognitive Science, Volume 3: Thinking*, chapter 3. MIT Press, Cambridge, Mass., second edition, 1995.

[Ste97] Helen Steward. *The Ontology of Mind: Events, States and Processes.* Clarendon Press, Oxford, 1997.

[Str97] B. Strauch. private communication. Jan 1997.

[Sve81] O. Svenson. Are we all less risky and more skillful than our fellow drivers? *Acta Psychologica*, 47:143–148, 1981.

[Swa00] Robert L. Swaim. Systems Group Chairman's Factual Report of Investigation. Technical Report Docket SA-516, Exhibit 9A, National Transportation Safety Board, Washington, D.C., August 2000.

[TEW90] M. Thompson, R. Ellis, and A. Wildavsky. *Cultural Theory.* Westview Press, Boulder, Colorado, 1990.

[TJ96] A.J. Telford and C.W. Johnson. Extending The Application Of Formal Methods To Analyse Human Error And System Failure During Accident Investigations. *Software Engineering Journal*, 11(6):355–365, November 1996. Available from `http://www.dcs.gla.ac.uk/ johnson/papers.html`, report TR-1996-6.

[TK81] Amos Tversky and Daniel Kahneman. The framing of decisions and the psychology of choice. *Science*, 211:453–458, 1981.

[TR76] R. Thaler and S. Rosen. The value of saving a life: Evidence from the labor market. In N. Terleckyj, editor, *Household production and compsumption*. Columbia University Press, New York, 1976.

[Uni90] United States Air Force. *AFR 127-4*. Author, 3 January 1990. This document in shortened form with slightly different numbering is also available as [Uni94].

[Uni94] United States Air Force. *Air Force Instruction 91-204*. Author, July 1994.

[U.Sa] U.S. Federal Aviation Administration. Airman's information manual. Published annually in full, updated bimonthly.

[U.Sb] U.S. Federal Aviation Administration. Airman's information manual, pilot/controller glossary. Published annually in full, updated bimonthly.

[U.Sc] U.S. Government, Federal Aviation Administration. 14 CFR Part [1 to 143, 830], Federal Aviation Regulations. Published annually in full, updated bimonthly.

[vdM00] M. van der Meulen. *Definitions for Hardware and Software Safety Engineers*. Springer-Verlag London Limited, 2000.

[VGRH81] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. *Fault Tree Handbook*. Number NUREG-0492 in Report. U.S. Nuclear Regulatory Commission, Washington, D.C., January 1981.

[Wei79] N. D. Weinstein. Seeking reassuring or threatening information about environmental cancer. *Journal of Behavioral Medecine*, 16:220–224, 1979.

[Wil79] R. Wilson. Analyzing the daily risks of life. *Technology Review*, 81(4):40–46, 1979.

[WS95] Richard H. Wood and Robert W. Sweginnis. *Aircraft Accident Investigation*. Endeavor Books, 1995.