Appendix A

EL Proof-Step Templates

A.1 The High-Level Template

Proving *causality* is a recursive procedure, that is, most steps have two substeps which are also assertions of $\Rrightarrow^*$. Eventually, however, the recursion must terminate with *base step* rather than a *recursion step*.

```
⟨1⟩1. $A \hookrightarrow B$
PROOF:
  ⟨2⟩1. $A \Rrightarrow^* B$
  PROOF:
    ⟨3⟩1. $A \Rrightarrow^* C$
    PROOF:
      ...
      ⟨4⟩1. $A \Rrightarrow^* D_0$
      PROOF:
        ⟨5⟩1. $A \Rrightarrow D_0$
        PROOF:
          ⟨6⟩1. $A \wedge D_0$
          PROOF:
            ⟨7⟩1. A
            PROOF: *********
            ⟨7⟩2. D$_0$
            PROOF: *********
            ⟨7⟩3. Q.E.D.
              ($\wedge$-introduction) from ⟨7⟩1 and ⟨7⟩2. □
          ⟨6⟩2. $\neg A \mathrel{\Box\!\!\rightarrow} \neg D_0$
          PROOF:
            ******Lewis semantics and possible worlds reasoning on $C$ and
            $D_0$******.
          ⟨6⟩3. Q.E.D.
```

Directly follows by Inference Rule 14.20 from ⟨6⟩1 and ⟨6⟩2. □

⟨5⟩2. Q.E.D.

Directly follows by Inference Rule 14.3 from ⟨5⟩1. □

...

⟨4⟩2. $D_0 \Rightarrow\!\!\!\succ^{*} D_1$

PROOF:

⟨5⟩1. $D_0 \Rightarrow\!\!\!\succ D_1$

PROOF: ******Similar to this step in ⟨4⟩1******

⟨5⟩2. Q.E.D.

PROOF:

Directly follows by Inference Rule 14.3 from ⟨5⟩1. □

...

⟨4⟩3. $D_n \Rightarrow\!\!\!\succ^{*} C$

PROOF: ******Similar to ⟨4⟩1******

...

⟨4⟩4. Q.E.D.

Directly follows by Inference Rule 14.3 from ....

...

⟨3⟩2. $C \Rightarrow\!\!\!\succ^{*} B$

PROOF: ******Similar to ⟨3⟩1**********

⟨3⟩3. Q.E.D.

Directly follows by Inference Rule 14.4 from ⟨3⟩1 and ⟨3⟩2. □

⟨2⟩2. Q.E.D.

Directly follows by Inference Rule 14.2 from ⟨2⟩1. □

A.2 Deontic Proof-Step Template

⟨1⟩1. $O(\Diamond \mathit{Event})$

PROOF:

⟨2⟩1. *Hypotheses*

PROOF: **********

⟨2⟩2. $(\mathit{Hypotheses} \land \Box \mathit{Procedures}) \succ \Diamond \mathit{Event}$

PROOF:

⟨3⟩1. $\vdash_{TLA} (\mathit{Hypotheses} \land \Box \mathit{Procedures}) \Rightarrow \Diamond \mathit{Event}$

PROOF:

FOLLOW: $\vdash_{TLA}$ rules only.

TLA*************TLA

⟨3⟩2. Q.E.D.

Directly follows by Inference Rule 14.21 from ⟨3⟩1. □

⟨2⟩3. Q.E.D.

Directly follows by Inference Rule 14.23 from ⟨2⟩2. □

A.3 CCT as a Derived Meta-Rule

⟨1⟩1. $C \Box\!\!\Rightarrow B$

PROOF:

⟨2⟩1. C

PROOF: ******

⟨2⟩2. $\neg C \Box\!\!\rightarrow \neg B$

PROOF:

⟨3⟩1. $\neg(A_1 \wedge A_2 \wedge A_3 \wedge ... \wedge A_n) \Box\!\!\rightarrow \neg B$

PROOF:

⟨4⟩1. $\neg A_1 \vee \neg(A_2 \wedge A_3 \wedge ... \wedge A_n) \Box\!\!\rightarrow \neg B$

PROOF:

⟨5⟩1. $\neg A_1 \Box\!\!\rightarrow \neg B$

PROOF:

*****

⟨5⟩2. $\neg(A_2 \wedge A_3 \wedge ... \wedge A_n) \Box\!\!\rightarrow B$

PROOF:

⟨6⟩1. $\neg A_2 \vee \neg(A_3 \wedge ... \wedge A_n) \Box\!\!\rightarrow \neg B$

PROOF:

⟨7⟩1. $\neg A_2 \Box\!\!\rightarrow \neg B$

PROOF: ******

⟨7⟩2. $\neg(A_3 \wedge ... \wedge A_n) \Box\!\!\rightarrow \neg B$

...

PROOF:

⟨8⟩1. $\neg(A_{n-1} \wedge A_n) \Box\!\!\rightarrow \neg B$

PROOF:

⟨9⟩1. $\neg A_{n-1} \vee \neg A_n \Box\!\!\rightarrow \neg B$

PROOF:

⟨10⟩1. $\neg A_{n-1} \Box\!\!\rightarrow \neg B$

PROOF: ******

⟨10⟩2. $\neg A_n \Box\!\!\rightarrow \neg B$

PROOF: ******

⟨10⟩3. Q.E.D.

Follows by Inference Rule 15.6 from ⟨10⟩1 and ⟨10⟩2. □

⟨9⟩2. Q.E.D.

Follows by De Morgan's law applied to the antecedent of ⟨9⟩1. □

⟨8⟩2. Q.E.D.

*****

⟨7⟩3. Q.E.D.

Follows by Inference Rule 15.6 from ⟨7⟩1 and ⟨7⟩2. □

⟨6⟩2. Q.E.D.

Follows by De Morgan's law applied to the antecedent of $\langle 6\rangle 1$. □

$\langle 5\rangle 3$. Q.E.D.

Follows by Inference Rule 15.6 from $\langle 5\rangle 1$ and $\langle 5\rangle 2$. □

$\langle 4\rangle 2$. Q.E.D.

Follows by De Morgan's law applied to the antecedent of $\langle 4\rangle 1$. □

$\langle 3\rangle 2$. Q.E.D.

Follows immediately by the definition of C.

$\langle 2\rangle 3$. $\neg B \mathrel{\Box\!\!\rightarrow} \neg C$

PROOF: ******

$\langle 2\rangle 4$. Q.E.D.

Directly follows by Inference Rule 15.5 from $\langle 2\rangle 1$, $\langle 2\rangle 2$ and $\langle 2\rangle 3$. □

Appendix B

Syntactic Definition of Textual WBGs in Extended BNF

We give the syntactic definition of the textual form of WB-Graphs in Extended Backus-Naur Form in Figure B.1.

```
textgraph   =  node {node}.
node        =  tag tag | tag node_ext node_info |
               tag “∧” node_ext node_info {“∧” node_ext node_info}.
tag         =  “⟨” path “⟩” | “[” path “]” | “{” path “}” | “(” path “)”.
node_ext    =  “⟨–.” number “⟩” | “[–.” number “]” | “{–.” number “}” |
                “(–.” number “)” |“⟪–.” number “⟫” | “⟦–.” number “⟧” |
                “⦃–.” number “⦄” | “⦅–.” number “⦆”.
node_info   =  “ /∗ ” descr [add_flags] “ ∗/ ”.
add_info    =  [“//#” fail_type“#”] {“//”add_flags}.

 path       =   number {“.” number }.
 number     =  digit | firstdigit {digit}.
add_flags   =  “@T” timestamp add_flags | “@A” number add_flags | descr_text.
timestamp   =  digit digit “ : ” digit digit “ ′ ” digit digit “ ″ ”.

anychar     =  char(0) .. char(127).
anytext     =  {anychar}.
descr       =  anytext EXCEPT .. “ ∗/ ”.. .
fail_type   =  “PERCEPTION” | “ATTENTION” | “REASONING” |
               “DECISION” | “INTENTION” | “ACTION”.
digit       =  “1” | “2” | “3” | “4” | “5” | “6” | “7” | “8” | “9” | “0”.
firstdigit  =  “1” | “2” | “3” | “4” | “5” | “6” | “7” | “8” | “9”.
```

Figure B.1: Textual WB-Graph Syntax representation in EBNF

Appendix C

Glossary

```
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
ATC      : Air Traffic Control
ATCC     : Air Traffic Control Center
ATS      : Auto-Throttle System
ATT      : Attitude
BATC     : Brussels Air Traffic Control
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
DH       : Decision Height
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
FI       : Flight Information (Flight data and Flight Plan)
```

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
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
LATC	: London Air Traffic Control
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
MDA	: Minimum Decision Altitude
MIC	: Microphone
MTP	: Maintenance and Test Panel
NAV	: Navigation
NPA	: Non Precision Approach
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
R ALT	: Radio Altitude
RET	: Retract
RMI	: Radio Magnetic Indicator
RWY	: Runway
SATC	: Shannon Air Traffic Control
SB	: Service Bulletin
SCT	: Scattered
SGU	: Symbol Generator Unit
SOP	: Standard Operating Procedure
SPD	: Speed
SPD/MAC	: Speed/Mach
SRS	: Speed Reference System
SW	: Switch
TCC	: Thrust Control Computer
TCD	: Ministry of Transport Civil Aviation Bureau Directive
TFC	: Traffic
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

Index

$[\mathcal{A}]_f$, 300
$\vee$-intro rule, 297
$\Rightarrow$-elim rule, 297
$\Rightarrow$-intro rule, 297
D_O axiom, 301
F axiom, 301
K axiom, 298
K_O axiom, 301
N_O rule, 301
P axiom, 301
$S4$ axiom, 298
$S5$ axiom, 298
T axiom, 298
VC logic, 304
VCU logic, 304
VCU-EL logic, 306
$\Box-$elim rule, 298
$\Box-$intro rule, 298
$\Box_C$, 304
$\Diamond$, definition, 101
$\bot_{\mathsf{c}}$ rule, 297
$\bot_{\mathsf{I}}$ rule, 297
$\exists-$elim rule, 298
$\exists-$intro rule, 298
$\forall-$elim rule, 297
$\forall-$intro rule, 297
STL1 axiom, 300
STL2 axiom, 300
STL3 axiom, 300
STL4 axiom, 300
STL5 axiom, 300
STL6 axiom, 300
STL7 axiom, 300
$\preceq_W$, 302
$\succ$, 215

INV1 rule, 300
INV2 rule, 300
TLA1 rule, 300
TLA2 rule, 300
$\Box\!\!\rightarrow$, Lewis semantics for, 212
ATCcomm_history module, 244
ATCcomm module, 243
ATCproc module, 242
ATCtrans module, 240
INJS resolution, INJSR, 149
PAD.ATCcomm_history module, 249
This_ATCcomm_history, 245, 246
chain conversion, CC, 149
$\vee$*-elim rule*, 297
AsNear relation, 306
Attend predicate, 268
CI-Script, 121, 123
CommProc principle, 217
Final approach phase, 280
Initial approach phase, 280
Landing_Axioms module, 325
Landing_Defs module, 324
Landing_Norms module, 327–329
Landing_Specs module, 330–334
Landing phase, 280
Mode module, 281
NavProc principle, 217
PARDIA-Norms module, 278
Perceive predicate, 268
Phases module, 280, 282
Proof-Obligations module, 372
RealTimeTheorems module, 322
Reason predicate, 266
SOP_Specs module, 336, 337
&-elim rule, 297

&-intro rule, 297
□⇒ , 222
accessibility relation, 306
accessible predicate, 306
cid2dot tool, 121
cid2ft, 137
dot tool, 121
landing mode, 280
nearer to, relation, 57
nearness relation, 306
wb2dot, 395

AAMP5 processor, 258
accident, 3, 8, 12, 16, 65, 66
accident, severity, 4
action, 206
action - PARDIA, 264
action failure, 265
adequate decomposition, 62
Air France administration, 178
Air Traffic Control Handbook, U.S., 227
alethic modality, 192
always-eventually property, 142
American Petroleum Institute, 6
Amp-hour, milli, 6
analysis, causal, 5, 13
analysis, risk, 8
analysis, technical risk (TRA), 11, 12
arc fault, 7
arc, electrical, 7, 9, 11
Arrow's Impossibility Theorem, 17
artifact, 3, 15
artifact, safety-critical, 12
ASRS, Aviation Safety Reporting System, 7
asymmetry, of nearness relation, 112
ATC, Air Traffic Control, 106
attention - PARDIA, 264
attention failure, 264
avalanche effect, 6
avionics, 7
avionics bay, see bay, 7

base station, mobile phone, 9
basic formula, 141
Basle-Mulhouse airport, 177
battery, phone, 5–7
bay, avionics, 7
Bayesian decision theory, 17
BBSTS principle, 11, 12, 14
behavior, 50, 53, 55
BMP, break multiple paths, 149
BMP, see Break Multiple Paths, 149
boundary assumption, 52
boundary, system, 50, 51, 67
Break Multiple Paths, BMP, 149
Brown, Simon, 5, 7, 8
Buga, Colombia, 381
Bunkley, Crawford, 9
Byzantine fault-tolerant algorithm, 257

cabin, aircraft, 7
Cali, Colombia, 381
catastrophic effect, 87
Causal Completeness Test, CCT, 219
causal factor, 190
causal factor, necessary, definition, 110
causal factor, relation, 117
causal field, 317
Causal Influence Diagram, CID, 121, 123, 137
causal mechanism, 11, 12
Causal Sufficiency Criterion, CSC, 219
Causal System Analysis (CSA), 49, 117
causality, true, 209
CC, see Chain Conversion, 149
CCT, see Causal Completeness Test, 219
certification basis, 87
CFIT, 67, 68
CFIT, controlled flight into terrain, 319, 381
Chain Conversion, CC, 149
change, 53
characteristic axiom, 306

Chicago Convention, 1948, 13, 105
CHIRPS, 7
CID, see Causal Influence Diagram, 121, 123, 137
Civil Aviation Authority, UK, 7
Class A mishap, USAF, 87
closed system, 107
closed-world assumption (CWA), 317
Coates, Mark, 8
cockpit voice recorder, 317
combustible substance, 5
Communications Advisory Panel, UK, 8
comparable worlds, 112
components, “programmable electronic”, 3
concomitant variation, 90
conductor, electrical, 6, 7, 11
Conflict Exit rule, 311
Conflict Remain rule, 311
Conflict Resolution rule, 310
conservatism, strong, 12
contact, battery, 6, 9, 11
contrastive explanation, 215, 226
contributing factor, 105
contributory factor, 190
correct fault tree, 140
correlation, 90
counteracting cause, 215
counterfactual, 109–111, 119, 120, 186
counterfactual conditional, 192
counterfactuals, logic of, 190
CRW, flight crew, 199
CSC, see Causal Sufficiency Criterion, 219
current, electrical, 9
CVR, cockpit voice recorder, 317
CWA, see closed-world assumption, 317

Dalton, John, 6
damage, 68
danger, 68
DATR programming language, 393
debugging, 195
debugging, as causal analysis, 113
decision - PARDIA, 264
Decision axiom, 280, 281
decision failure, 264
decision problem, 19
Decision Science, 17
deontic modality, 192
deontic operator, 267
deontic reasoning, 215
Deontic rule, 216
deontically-correct world, 227
DEPOSE classification scheme, 62
DF, Don’t Fret, 12, 14
DF, Don’t Fret principle, 12
DFDR, digital flight data recorder, 317
diachronic contrast, 226
Difference Condition, 197, 226, 384
digital flight data recorder, 317
discharge, electrical, 7
discrete factor, 119, 122
discrete sequence, 55
disjunctive normal form, DNF, 141
distributed system, 195
DNF, see disjunctive normal form, 141
domain, of a relation, 94
Douglas, Mary, 20, 21
DU (don’t use), 11

EL Behavioral Rules, 310, 311
EL logic, 140, 192
EL Special Rules, 308, 309
entry/exit conditions, 279
environment, 50
Ericsson, 6
escape manoeuvre for GPWS, 382, 383
event, 55, 206
event type, 55, 88, 206
extremely improbable event, definition, 86

extremely remote event, definition, 86

failure, 66
failure analysis, 195
far change, 56
FAR, see Federal Aviation Regulations, 227
fault tree, 127, 137
Fault Tree Analysis, FTA, 17, 127
FDR, flight data recorder, 178
Federal Aviation Administration, U.S., 177
Federal Aviation Regulations, U.S., 86, 194, 227
field strength, electromagnetic, 5
field, electrical, 7
fire, 5
flight deck, 7
Flight Management Computer, FMC, 382
flight phases, 279
fluent, 53
FMC, see Flight Management Computer, 382
forecourt, gas station, 3, 5, 7–9
formalism, 49
freedoms, infringement of basic, 12
frequent event, definition, 86
fusion, 59

Galbraith, John Kenneth, 12
Ganter, John, 5, 9
gas law, 119, 120
go-around mode of autopilot, 423
goal, 15, 16
group, lobbying, 15
group, special interest, 15
Guidance, Home Ofice HGN(F)15, 8

Höhl, Michael, 176
Habsheim A320 accident, 175
hazard, 3, 4, 8, 9, 12, 68, 102
hazard condition, 118
hazard level, 68
hazard, latency, 4
Hazard-1, definition, 71
Hazard-1, intuition, 85
Hazard-2, definition, 71
Hazard-2, intuition, 85
Hazard-3, definition, 72
Hazard-4, definition, 72
Hazard-4, intuition, 86
Hazard-5, definition, 73
hazardous airspace, 67
hazardous effect, 87
Hazop (Hazard and Operations Analysis), 17
Health and Safety Execituve, U.K., 5
Health and Safety Executive, U.K., 3, 6, 12
heterogeneous system, 107, 195
higher-order type theory, 54
Highway Code, U.K., 8
history, 207
history variable, 54
Hume, David, 109, 186, 208
hybrid system, 195

ICAO, see International Civil Aviation Organisation, 13, 105, 227
IFIP Working Group 10.4, 87
ignition, 8
ignition, fuel, 6
ignition, of fuel/air mix, 5
immunity, electromagnetic interference, 7
improbable event, definition, 86
Inconsistency rule, 310
independence, probabilistic, 4
information processing model, 193
information-processing model, 263, 273
INJS factor, 144
INJSR, INJS resolution, 149
Institute of Petroleum, UK, 8
intensional context, 221
intensity, electromagnetic field, 7
intention - PARDIA, 264

intention failure, 264
intention, human, 15
interactive complexity, 106
interactively complex system, 62
interactively coplex system, 62
interference, electromagnetic (EM), 7
interlock, 110
International Civil Aviation Organisation, ICAO, 13, 105, 227
inverse natural deduction, 339
Irish Aviation Authority, 200
irreflexivity, of nearness relation, 112

Johnson, Chris, 208
Joint Aviation Regulations, European, 86
Jones, Jim, 21
Jonestown massacre, 21
Joule, milli (mJ), 6, 7

Know and Consult principles, 17
Kripke semantics, 210

Lamport, Leslie, 188
Landing procedure state predicates, 335
latency, hazard, 3, 68
levels of analysis, 116
Leveson, Nancy, 24, 66, 67, 188
Lewis, David, 109–112, 140, 180, 186, 226
life, monetary value of, 13
likelihood, accident, 4
likelihood, conditional, 4
likelihood, hazard, 4, 68
LIL (like is like), 11
LIL (Like is Like) principle, 11, 12, 14
Lipton, Peter, 226
liveness property, technical, 140
logic, applied formal, 47
loose coupling, 106
loss, 4, 20
loss, expected, 4

Mackie, John, 316
major effect, 87
MEC, see Minimise Expected Cost principle, 13
mereological sum, 60
mereology, 59
Method of Differences, Mill's, 7, 226
Methods of Induction, Mill's, 230
mid-air collision, 88
MIL-STD-882, 72
Mill, John Stuart, 7, 90, 109, 186, 197, 208, 215, 226
Minimise Expected Cost principle (MEC), 13
minor effect, 87
Minuteman ICBM system, 137
mix, fuel-air, 7, 11
MJ (Multiple Justification), 11, 12, 14
mJ, see Joule, milli, 6, 7, 462
modality, counterfactual, 13
mode confusion syndrome, 279
mode, phone standby, 9
Moffett, Jonathan, 208
money, namely $ 10,000, 20
Motorola, 6
MPR Iteration, MPRI, 148
MPR, see Multiple Path Reduction, 148
MPRI, see MPR iteration, 148
Multiple Path Reduction, MPR, 148
myth, urban, 5

N1, engine measure, 178
Nagoya, Japan, 423
narrative of accident, 409
National Public Radio, U.S., 5
National Research Council, Committee on Risk Characterization, 22
National Transportation Safety Board, U.S., 177, 382

NCA, see necessary causal ancestor, 145
near change, 56
nearness relation, 111, 210
necessary causal ancestor, NCA, 145
necessary causal factor, NCF, 143
necessary implication, 192
negatively causally dependent, 120
neolithic causal regularity, 230
node, 206
noise, electromagnetic (EM), 7
Nokia, 6
non-event, 206
Northwest Airlines, 200, 205
NRC, see National Research Council, 23

object, 50
object, atomic, 73
object, environment, 93
object, system, 93
object, world, 93
objective judgement, 189
OHRS, open heterogeneous real-time system, 195
open system, 107, 195
ordinal measure, seeordinal scale, 302
ordinal scale, 58, 302
Ought - see deontic operator, 266
overcounting, 83, 84
oxygen, 5

PAD, see predicate-action diagram, 233, 247
paradoxes of belief, 269
paralysis, social, 12
PARDIA, 263
PARDIA axioms, 271
PARDIA classification, 192, 193
PARDIA norms, 272
part, of object, 58
part, structural, 59
path, causal, 14
PC (prior coverage), 12, 14
PC (prior coverage) principle, 11, 12, 14
PCJ (Physical Causal Justification), 12, 14
PED (personal electronic device), 7
perception - PARDIA, 264
perception failure, 264
Perrow, Charles, 62, 63, 105–107, 185
Petroski, Henry, 185
phone, mobile, 3, 5–9
pilot, as aircraft part, 105
policy, public, 8
policy, safety, 8
positive Boolean expression, 138
positively causally dependent, 120
possible world, 304
Prawitz, Dag, 295
precautionary principle, 11
predicate, environment, 94, 95
predicate, hybrid, 94, 95
predicate, system, 94, 95
predicate-action diagram, PAD, 233, 247, 256
Preface Paradox, 269
preorder, total, 211
pressure tank, CSA example, 115
pressure, air, 6
probability, 76
probability, conditional, 4
probable cause, 105, 190
probable event, definition, 86
procedural conflict, 289
process, 206
process, "analytic-deliberative", 23
proof obligations, 372
prophylaxis, 89

Qualitative Physics, 120

radiator, electromagnetic (EM), 5
radio, CB, 9
rational choice, 17

RCBA, Risk Cost-Benefit Analysis, 13, 21, 22, 41
reasonably probable event, definition, 86
reasoning - PARDIA, 264
reasoning failure, 264
reasoning, failure, 60
reasoning, inductive, 17
reflexity property, 211
relatively sufficient causal explanation, 192
reliability, 65, 66
remote event, definitions, 86
rigor, 49
risk, 4, 12, 15
risk analysis, 12
Risk Analysis journal, 13
risk assessment, 16, 17
Risk Cost-Benefit Analysis (RCBA), 13, 21, 22, 41
risk, acceptable, 18, 19
risk, characterisation, 22
risk, definition of, 68
risk, fact and value separation, 18, 21
risk, knowledge and consent criteria, 20
Royal Society, 22
ROZO One arrival to Cali, 382

safety, 65, 66
safety analysis, 3
safety property, technical, 140, 141
Sagan, Scott, 106
Schepper, Willi, 6
semi-component of a graph, 414
servant, 11
severity, 4, 20
severity, accident, 3, 4
severity, hazard, 68
short circuit, 7
Siemens, 6
SO (switched off), 11
SOP, Standard Operating Procedures, 194, 326
sound causal explanation, 192
source, ignition, 5
spark, 5, 7, 9
spark, incendive, 6, 9
standard, BS 6656:1991, 5
standard, BS 6941:1991, 10
standard, IEC 61508, 3
stasis, 118
state, 53, 54, 205
state description, 53
state, environment, 95
state, hybrid, 95
state, system, 95
state, world, 95
stealing, sheep, 20
Steward, Helen, 418
stopping constraint, 101
Strauch, Barry, 399
strict implication, 215
sufficient causal factor, SCF, 143
sufficient cause, 192
sufficient explanation, 219
sufficient set of causal factors, 219
superfluous nodes, in fault tree, 155
surge, electrical, 7
Sweginnis, Robert, 187, 209
symmetry property, 211
system, 3
system accident, 106
System S, 74
system, predator-prey, 15
system, social, 15
system, teleological, 15, 16, 19, 44, 51

technical risk analysis, 13
temporal extent, 207
temporal logic, 140
temporal strengthening, 118
tense-logical operator, 101
terminal, battery, 6, 7
Thimbleby, Harold, 6

tight coupling, 106
tightly coupled system, 62
TLA+ specification language, 192, 233
TLA, the Temporal Logic of Actions, 188
TOGA, Take-off/Go-around thrust, 178
token, 59
totality property, 212
TRA, see analysis, technical risk, 13, 14
TRA, Technical Risk Analysis, 14
TRA, technical risk analysis, 13, 14
transitive closure of a relation, 112, 190
transitivity property, 112, 211
transmission, Radio Frequency (RF), 9, 11
transmitter, Radio Frequency (RF), 8
TRAV, Technical Risk Analysis Validity, 13, 14

U.S. Air Force, 87, 110
undercounting, 84
undercounting problem, 84
Uniformity Condition, 306
universum, definition, 52, 73

value-influence factor, 120, 122
vapor, flammable, 5, 8
VCU logic, 192
Venn diagram, 50
Volt, 6
Volts/meter, 7

Warsaw A320 accident, 175
weak order, 211
Why-Because Analysis (WBA), 50
Wildavsky, Aaron, 20, 21
Wood, Richard, 187, 209

Zermelo-Fraenkel set theory, 54