

Causal System Analysis
Formal Reasoning About Safety and Failure

Document RVS-Bk-01-01

DRAFT Version 2.0

©1998, Peter B. Ladkin and Karsten Loer, 2000, 2001 Peter B. Ladkin

Peter B. Ladkin
Faculty of Technology, University of Bielefeld
`ladkin@rvs.uni-bielefeld.de`

August 14, 2001

Preface

Systems in computer science have long been analysed using mathematics and logic, so-called formal methods. Although progress may have seemed slow in comparison with progress in building systems themselves, it is maybe generally to be expected from the history of technology. Amongst the advantages of formal methods are precision, explicitness, and objectivity. When formal methods are used, it is not longer a matter of individual judgement whether something works, or some property is satisfied, but a public matter. Everyone must in principle reach the same conclusion (modulo technical knowledge of the method) when the analysis is presented. That means that analyses can be criticised, and problems become objective, no longer a matter for intuitive judgement alone. Critiques may be discussed amongst a broader competence group, and this has long been recognised as an advantage for the accuracy of sensitive judgements on reliability and safety. The disadvantage of formal methods, to my way of thinking, lies predominantly in their complexity, and the degree of technical mathematical sophistication required of their users, who are mostly engineers without advanced mathematical training.

Safety and failure analyses, such as those of accidents, have long involved individual engineering judgement in most if not all aspects. This book introduces formal methods for such analyses, and I hope thereby to bring the advantages to bear on this engineering discipline. Avoiding the disadvantages is a little more problematic. There will always be a certain level of complexity and technical sophistication required of users of a rigorous method. But one may also hope for a less-formal procedure which will suffice to bring many of the advantages of objectivity and explicitness, while suffering from fewer of the disadvantages of complexity and intellectual inaccessibility.

Causal Systems Analysis (CSA) is a formal method for performing a priori safety analyses of complex, open, heterogeneous technical systems. It also comprises the Why-Because Analysis (WBA) method for a posteriori safety analysis, the analysis of failure incidents and accidents. The methods are based upon a formal notion of causality espoused by David Lewis.

Lewis's definition of causality has both semantic and syntactic formulations. The semantic formulation allows one to determine whether one event or state causally affects or affected another, through considering how the world might

have been, had one or the other not occurred. Such considerations are part of the so-called “possible worlds” semantics for formal logics with modalities, but they also lend themselves to intuitive “what if” judgements about the world we live in. These intuitive judgements I call the “informal semantics”. Lewis proposed a complete axiomatic formulation of his notion of causality, in the form of a formal logic with a causal modality.

Physical systems are mostly constructed with an eye to causality: one builds such a system so that certain desired effects are deliberately caused by various components. It makes sense to analyse such systems through determining the causal influences amongst the components. Safety analysis is concerned not just with how things happen when they go right, but what can happen when they go wrong. Either way, the behavior has a large, if not predominant, causal component. Lewis’s analysis of, and semantics for, causal notions lends itself to this task, because of its formal underpinnings as well as its informal semantics.

Chapter 1 motivates technical risk analysis, through an example of how technical risk and safety are often dealt with at the level of society. Chapter 2 illustrates some aspects of thinking about risk, including psychological and social-psychological factors, as well as attitudes enshrined in professional engineering codes of conduct.

Chapter 3 sets out the basic technical material for CSA: the ontology and fundamental concepts. Definitions follow in Chapter 4. Chapter 5 sets out some conceptual problems with some safety definitions in common use, through consideration of a simple example in which none of them appear to work as intended. Chapter 6 brings some of the methods of formal logic to bear on the language of systems, and Chapter 7 illustrates the use of the material introduced so far on a simple game of golf. After a further introduction of technical machinery in Chapter 8, Chapter 9 introduces Causal Systems Analysis itself, on the well-worn example of a pressure tank. Chapter 10 shows how a Causal Influence Diagram, the result of a CSA, may be converted automatically into a fault tree, the staple of engineering safety analysis tools.

Chapter 11 motivates the accompanying failure-analysis method, Why-Because Analysis, through performing a high-level WBA of two high-profile commercial aviation accidents, the 1988 accident to an Air France A320 at Mulhouse-Habsheim, and the 1992 accident in Warsaw to a Lufthansa A320. Background material and technical motivation occupies Chapter 12, and typical short aviation incident reports are presented in Chapter 13. The presentation of Why-Because Analysis properly starts in Chapter 14, using a running example gleaned from one of the short incident reports presented earlier. Chapters 15, 16 and 17 complete the exposition of WBA on the running example.

It remains to be shown that the causal analysis derived in the previous chapters satisfies the explicit correctness and sufficiency criteria for such an analysis. The next few chapters show how a formal proof of correctness and relative sufficiency of a causal explanation produced by WBA proceeds. Chapter 18 includes

the human-agency classification method PARDIA, along with its formal axiomatisation. This is followed in Chapter 19 by an explanation of how flight procedures and phases are axiomatised. The formal causal logic, Explanatory Logic or EL, is introduced in Chapter 20. The procedures relevant to the correctness proof of the causal explanation of the running example in Part IV are axiomatised in Chapter 21 and the proof of correctness and relative sufficiency of the explanation is presented in Chapter 22.

I emphasised earlier the importance of informal methods to accompany formal analyses. Three informal analyses of commercial aviation accidents are presented in the remaining Chapters 23, 24 and 25 to illustrate how WBA may be used in everyday engineering analysis of failure. In two of these three examples, we discovered problems with the conclusions of the reports concerning the “probable cause” and “contributory factors” of the accidents. The discovery of the problems, and the confirmation that these are indeed problems, illustrates the earlier point concerning objective analysis methods and the advantages of more-public analysis and discussion of incidents.

Many people have been involved in the development of WBA and CSA. Karsten Loer and I worked together on a daily basis for six months, as I developed the required logic and he applied it to the formal proof of correctness and relative sufficiency of the running example, which proof became his Diplomthesis at the University of Bielefeld. Parts III and IV were written jointly with Karsten. His work was fundamental to the development of WBA. Besides performing the informal analysis of the Warsaw accident in WBA with me, Michael Höhl produced many of the illustrations in this book, and wrote the software that translates *WB-Script* and *CI-Script*, passes them through the *dot* graph-drawing tool, and produces the CIDs and WBGs which illustrate this book. These tools are also offered as a service on our WWW-server. Thorsten Gerdsmeyer worked with Karsten and myself on the first WBA, that of the Cali accident. Bernd Sieker and Joachim Weidner codeveloped the translation of CIDs into fault trees, and Bernd wrote the software, *cid2ft*, which presents the fault trees in graphical form. This tool is also offered as a service on our WWW-server. Finally, two behind-scenes contributors. Heiko Holtkamp has been instrumental in formatting and designing the presentation of the graphics that accompany Causal System Analyses and Why-Because Analyses, as well as preparation of our diagrams for posters and computer-mediated presentations of our work. Marcel Holtmann has configured and run the computer systems that constitute the `rvs.uni-bielefeld.de` net, as well as designing the layout of our WWW pages. All of these people have been essential to the material in this book.

Finally, preparation of this book started nearly four years ago around the birthday of my son, Simon Retzlaff. Both have grown a lot. He has enriched my life in the last four years in a way which I had not previously imagined. Simon, this book is for you, with thanks.

Contents

Preface	iii
I Introduction: The Social Background	1
1 An Example of Everyday Technical Risk Analysis	3
1.1 Engineering Risk Analysis	3
1.2 Phones on Forecourts: Causal Analysis	5
1.3 Phones on Forecourts: Safety Policy	8
1.4 Some Principles	11
2 The Social Background to Technological Risk	15
2.1 What Is Risk?	15
2.2 Risk And Teleological Systems	15
2.2.1 Risk Analysis As Profession	16
2.3 Risk Assessment	17
2.3.1 Two Principles: Know And Consult	17
2.3.2 Fact And Value	18
2.3.3 “Acceptable Risk”: A Confused Concept?	18
2.3.4 Risk As Decision	19
2.4 Alternative Conceptions of Risk	20
2.4.1 Risk as Interplay of Knowledge and Consent	20
2.4.2 The Royal Society’s View	21
2.4.3 The National Research Council’s View	22
2.4.4 A Software Safety Expert’s View	24
2.4.5 Risk Decisions As A Feedback System	24
2.4.6 Perception is an Irreducible Component of Risk	25
2.4.7 Risk Compensation	26
2.4.8 Summary: Risk As Cultural Artifact	28
2.5 Cultural Theory	28
2.5.1 Attitudes to Nature and Risk	28
2.6 Perception Heuristics	33
2.6.1 Problem Presentation Affects Choice	33

2.6.2	Prospect Theory	34
2.6.3	Other Heuristics	34
2.7	Difficulties With the Numbers	37
2.7.1	An Example: The Value of a Life	37
2.7.2	Example: Cigarette Smoking Deaths	37
2.8	Excessive Prudence Is Disadvantageous	38
2.9	How Biases May Affect Assessments	38
2.9.1	Cultural Biases	38
2.9.2	Evaluation Biases	39
2.9.3	An Example: Negotiating a Smoke	39
2.10	Professional Attitudes To Risk Management	40
2.10.1	Engineering Codes of Ethics and Their Consequences	40
2.10.2	An Example of What Counts: The Therac-25	41
II	Causal System Analysis	45
3	The Foundations of System Analysis	47
3.1	Preliminaries: The Importance of Reasoning	47
3.2	Formal Causal System Analysis	49
3.3	What is a System?	50
3.4	Objects and Fluents	53
3.5	State, Events and Behavior	53
3.6	Objects, Parts and Failure Reasoning	58
4	Definitions for System Safety Analysis	65
4.1	Reliability and Safety	65
4.2	Definitions of Safety Concepts	66
5	Problems Calculating Risk Via Hazard	71
5.1	Five Notions of Hazard	71
5.1.1	The System Safety and Associated Notions	71
5.1.2	The MIL-STD-882 Definition: Hazard-5	72
5.2	Definition of the System S	73
5.3	Calculating Hazard-4 and Hazard-1 States	75
5.3.1	Identifying The Hazard-4 States	75
5.3.2	Identifying the Hazard-1 States	76
5.3.3	An Accident Without a Preceding Hazard	76
5.4	Calculating Probabilities	76
5.5	Calculating Hazard-3 and Hazard-5 States	80
5.5.1	Determining the Hazard-5 States	80
5.5.2	Determining the Hazard-3 States	81
5.6	The Calculation of Risk Via Hazard	82

5.7	The Problem	83
5.7.1	The Risk of Overcounting	83
5.7.2	Not All Accidents Occur Through Hazards	84
5.7.3	Summary	84
5.8	Trying To Fix It	84
5.9	Motivating The Conceptions of Hazard	85
5.9.1	Weakening the Inevitability Requirement	86
5.9.2	Avoidance Of The Problematic Notions	87
5.9.3	Classifying Risk Through Statistics	87
5.10	Summary	91
6	More Theory: Types of Predicates	93
7	An Example: Playing Golf	97
7.1	The Basics: Objects, Predicates, Accident	97
7.2	The System And Behavior	98
7.3	Expressing Constraints on Behavior	100
7.4	Hazard Definitions and Consequences	102
8	Some More Conceptual Machinery	105
8.1	System Properties in the Large	105
8.2	Causality	109
8.2.1	Hume	109
8.2.2	The U.S. Air Force	110
8.2.3	Lewis	110
8.2.4	Aside: Causality and Computers	113
9	Causal Analysis of a Pressure Tank	115
9.1	Basic Concepts: Object, Properties, Relations	115
9.2	Causal System Analysis (CSA)	117
9.3	The Causal Influence Diagram	121
9.3.1	Generating the CID from CI-Script	121
9.3.2	Analysing the CID	122
9.3.3	Analysing The Modified System	123
9.3.4	Causal System Analysis of the Vent Subsystem	125
10	Generating Fault Trees from CIDs	137
10.1	Some Considerations on Fault Trees	137
10.1.1	How Fault Trees Look	137
10.1.2	The Logical Structure of Fault Trees	138
10.2	Why Generate Fault Trees Automatically?	141
10.3	A Causal Influence Diagram Example	143
10.4	Denoting “Normal” and “Failure” Conditions	144

10.5 Handling the Individual Components	145
10.6 Putting It All Together	148
10.7 A Simplified Fault Tree	154
10.7.1 Handling Superfluous Nodes	155
10.8 Implementing Fault-Tree Generation	155
10.8.1 Labelling the Fault Tree Nodes	155
10.8.2 The Logical Generation of Labels	159
10.8.3 A Second Example	163
III Why-Because Analysis	
(with Karsten Loer)	173
11 Accident Analysis: Why-Because Analysis	175
11.1 A WB-Analysis of the 1993 Warsaw A320 Accident	175
11.2 The 1988 Habsheim Accident	177
11.3 Conclusions	180
12 What It's All About	185
12.1 The State of the Art	185
12.2 Making the Reasoning Rigorous	189
12.3 The Development of WBA	190
12.4 Some Properties of WBA	191
12.5 Failure Analysis as Formal 'Debugging'	195
13 Aviation Incident Reports	199
13.1 Three Reports of the Example Incident	200
13.1.1 DC-10 misses Frankfurt runway – by 300km	200
13.1.2 Fly NorthWest Airlines to unknown destinations	201
13.1.3 Re: Fly NorthWest Airlines to unknown destinations	201
13.2 Typical History Summaries (Peter Mellor)	202
13.2.1 26th June 1988, Mulhouse-Habsheim in eastern France. Air France A320-100, registered F-GFKC	202
13.2.2 5th December 1989, Lille, France Air Inter, A320 (type not given), registered F-GHQB Private aircraft, Mooney, registered PH-WJO	203
13.2.3 14th February 1990, Bangalore, India. Air India, A320- 231, registered VT-EPN	203
13.2.4 20th January 1992, Strasbourg in eastern France Air Inter, A320-111, registered F-GGED	203
13.2.5 14th September 1993, Warsaw, Poland Lufthansa, A320- 200, registered D-AIPN	203

14 A WBAnalysis	205
14.1 The Ontology	205
14.2 First, Determining a Temporal Succession	207
14.3 Rules for Causality	208
14.4 Proving Causal Dependency	210
14.4.1 The Mathematical Semantics	210
14.4.2 Causes from Counterfactuals	212
14.5 Finding Causal Candidates	212
14.6 Non-Events and Deontics	215
15 Sufficient and Contrastive Explanation	219
15.1 Sufficient Causal Explanation	219
15.1.1 The Causal Sufficiency Condition	219
15.1.2 The CCT for [11] and [12]	220
15.1.3 Inference Rules for the CCT	222
15.1.4 Causal Sufficiency Through Procedural Necessity	223
15.1.5 The Next Step	226
15.2 Contrastive Explanation	226
15.2.1 Proceeding by determining earlier contrast	227
15.2.2 Mill's Other Methods	230
16 Specifying ATC Procedures	231
16.1 Introducing TLA+	233
16.2 Physical Subsystems	237
16.2.1 Inter-ATC Communication	237
17 Indeterminacy and the Endgame	247
17.1 Logical Analysis of Handover Failures	247
17.1.1 Defining the PAD Rigorously	247
17.1.2 Detecting possible sources of error	248
17.1.3 Putting all the Pieces Together	252
17.2 The Endgame	252
17.2.1 Constraining the Hypotheses	253
17.2.2 Indeterminacy	253
17.2.3 Adapting PADs	256
17.3 The Really Final WB-Graph	257
IV Formal Proof of WBA Correctness (with Karsten Loer)	261
18 The PARDIA Classification	263
18.1 Analysis of Pilot Behavior	263

18.2	A Tricky Example	265
18.3	Perception and Attention	268
18.4	Why Epistemics Are Not Included	269
18.4.1	Some Apparent Paradoxes of Belief	269
18.4.2	Allowing for Belief	270
18.5	PARDIA Axioms as a Module	271
18.6	PARDIA Norms	272
18.6.1	Intentions and Deontics	272
18.7	“Human Subsystems” - PARDIA	273
18.7.1	The Classification Scheme	273
18.7.2	Specifying the PARDIA Model	274
19	Flight Phases and System Modes	279
19.1	An EL Rule for Required Decisions	284
19.2	An Unsatisfactory Rule	285
19.3	Justification for the Behavioral Rule	287
19.4	Separating Two Steps	288
19.5	Procedural Conflicts	289
19.5.1	Determining Rules for Behavior	291
20	The Logic EL	295
20.1	Classical Rules	295
20.1.1	Propositional Rules	297
20.1.2	Quantifiers	297
20.2	Modal Rules	298
20.3	Temporal Rules	299
20.4	Behaviors and the Rules They Engender	300
20.5	Strict Implication	300
20.6	The Deontic Modalities	301
20.7	Lewis Semantics for Counterfactuals	301
20.8	Rules for Counterfactual Conditionals	303
20.9	Defining the Other Modalities	304
20.10	Causal Sufficiency	305
20.11	The Well-Formed Formulas of EL	305
20.12	Soundness and Completeness Observations	306
20.13	Special EL Rules	307
20.14	Axioms and Processes for WBA	313
20.15	VCU-EL Semantics Illustrated	314
20.16	Extensions and Modifications	316
20.16.1	Giving Priority to Causal Factors	316
20.16.2	Closed World Assumptions	317
20.16.3	Other Non-Monotonicity	317
20.16.4	Casual Defeasibility	318

20.16.5 Summary	319
21 Procedure Specifications in TLA+	321
21.1 Real Time Theorems	321
21.2 Procedures	323
21.2.1 Specification of Landing Procedures	323
21.2.2 Standard Operating Procedures	326
22 Formal Proof of Explanation	339
22.1 The Hierarchical Proof-scheme	339
22.2 Sufficient Causal Explanation Proof	340
22.2.1 Proof of [1]	341
22.2.2 Proof of [11]	343
22.2.3 Proof of [111]	346
22.2.4 Proof of [1111]	348
22.2.5 Proof of Node 12	354
22.2.6 Proof of (121)	356
22.2.7 Proof of Node 2	362
22.2.8 Proof of Node 22	366
22.2.9 Proof of Node 3	368
22.2.10 The Full Explanations	372
22.3 The Final WB-Graph	375
V Less-Formal WBA of Important Incidents	379
23 The Cali Accident	381
23.1 The Accident	382
23.2 The Cali Report	382
23.3 Linguistic Analysis of Pilot/ATC Communications	384
23.4 The Textual Version of the Cali WB-Graph	387
23.5 Finding and Resolving Discrepancies	392
23.6 Automated WB-Graph Construction and Checking	393
23.7 ‘Processes’ – Event/State Ambiguity	394
23.8 The Cali WB-Graph Layout	395
23.9 Source Nodes in the WB-Graph	397
23.10 Critique	398
23.11 Discriminating the ‘Significant’ Events	399
23.12A Comparison with the Cali Conclusions	401
23.13 Conclusions from the WB-Graph Construction	403
23.14 The Cali Report Conclusions	403

24 The 1993 Warsaw Accident	409
24.1 The Background	409
24.2 The Narrative	409
24.3 Analysis of the Narrative	411
24.4 The WB-Graph	411
24.5 The Textual Form of the WB-Graph	411
24.6 The WB-Graph and its Semi-Components	414
24.7 The Source Nodes	414
24.8 Conclusions	417
24.9 Causal Factors are Numerous	418
25 The WB-Graph of the 1994 Nagoya Accident	423
A EL Proof-Step Templates	449
A.1 The High-Level Template	449
A.2 Deontic Proof-Step Template	450
A.3 CCT as a Derived Meta-Rule	451
B Syntactic Definition of Textual WBGs in Extended BNF	453
C Glossary	455
