Causal System Analysis
Formal Reasoning About Safety and Failure

Document RVS-Bk-01-01

DRAFT Version 2.0

Peter B. Ladkin
Faculty of Techology, 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 Gerdsmeier 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