CAFOS - THE COMPUTER AID FOR OPERABILITY STUDIES

MC Jones(*) and DA Lihou(**)

The computer aid for operability studies (CAFOS) transforms hazard and operability studies in the form of cause and symptom equations, into pictorial fault trees, and provides rapid calculation of probabilities in the fault trees. The paper discusses: (i) rules for generating cause and symptom equations; (ii) a database for uncertain primary event probabilities and (iii) heuristics for dealing with repeated events in the fault trees. Two examples, illustrating qualitative and quantitative uses of the computer package, led to the conclusion that rapid probability evaluation was the main benefit from CAFOS.

INTRODUCTION

The need for hazard and operability studies is the same for processes designed with computer aids as for conventionally designed processes, but the possibility of automating the analysis is greater with CAD designs for two obvious reasons; (1) the user of CAD designs has computer hardware and VDU displays at his finger tips, and (2) the logical representation of the process to be analysed is, at least in principle, available directly from the CAD output.

The computer aid for operability studies (CAFOS) is a computer package designed to transform hazard and operability analyses expressed in the form of Cause and Symptom Equations (1), into pictorial fault trees, and to enable rapid calculation of event probabilities in the fault tree from a databank of primary events probabilities.

This paper outlines the structure of CAFOS, the input data required, and illustrates its output and usefulness with two examples of operability studies carried out by using CAFOS.

OPERABILITY STUDIES

The use of operability studies to review process designs for malfunctions is well established. Coded records have been used by Lihou (1, 2, 3) to speed and systemise the results of the studies. The coded results are expressed as;

Cause equations in which a deviant state ("event") is equated to the combination of events that cause it.

Symptom equations where a deviant state is related to the events that will result from it.

*Chemical Engineering Department, Aston University, Aston Triangle, Birmingham B4 7ET
** Lihou Loss Prevention Services Ltd, Science Park, Aston Triangle, Birmingham B4 7ET.

In the analysis of process P and I diagrams, cause equations usually relate down-stream states in process lines to their upstream precursors and symptom equations connect states at the imputs to vessels to the resulting output states.

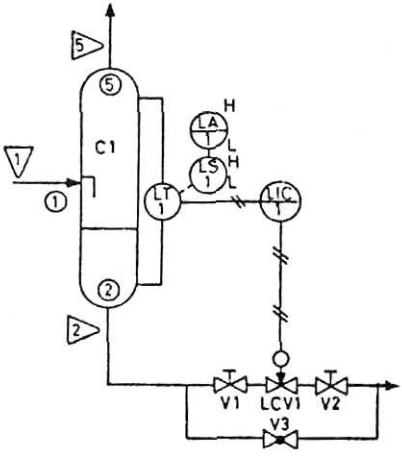
Figure 1 shows examples of the 2 kinds of equations for a simple process vessel and its connected lines. Conversion of the verbal form of the equations to the coded version used the translation table given in Table A1-1, Appendix 1.

Formation of cause and symptoms equations by an operability study team is a skilled and lengthy exercise, and the results may be hard to interpret as they stand, requiring pictorial and quantitative treatment before they have meaning to the process analyst. The construction of fault trees from hazop results and their analysis is a well established technique, recently reviewed in detail (4), but the design engineer cannot be expected to carry out the technique unaided. CAFOS is the first of a set of packages developed to aid in the performance and interpretation of operabilty studies. It is designed to produce rapid pictorial fault trees from existing cause and symptom equations, to quantify the fault events by automatic calculation of their probabilities, and hence focus on the significant fault states and on design changes to reduce their occurence.

RULES FOR CAUSE AND SYMPTOM EQUATIONS

Cause and symptom equations, or other forms of operability study records, must at present be generated by an operability study team who may spend many hours on a single P and I diagram, making the study a significant expense in the design process. There is considerable interest in formulating rules to speed up the analysis. Lihou (5) has given a classified set of rules of which Figure 2 is a simple example.

Figure 1 Cause and Symptom Equations



(1) Considering causes of no flow in line 2, we could write:

(no flow, line 2) caused by (no flow into line 2)
or (line 2 blocked)
or (line 2 valves blocked)

This Cause Equation has the coded form:

L1(11) = N2(11) + L2(0) + L2(BV).

(2) Considering consequences of no flow into the vessel C1 which has inlet and outlet nodes named N1 (node where line 1 enters), N2 and N5:

(no flow at node 1) causes (no flow at node 2) and (no flow at node 5).

This Symptom Equation has the coded form:

N1(11) - N2(11) *N5(11).

(Note the use of the operators "=", "-", "+", "*" to distinguish cause and symptom equations, and alternative and conjoint logic).

Figure 2 An Example of CAFOS Rules

"Pipelines - Flow

Index No 1 No flow may be caused by any of the following:-

* No flow in the line(s) immediately upstream
* No flow at the node where the line leaves an equipment
* The supply tank empty
* A valve shut in the line
* A filter fully blocked in the line
* A pump in the line stopped"

The existence of such rules, which have been usefully employed to deduce correct cause and symptom equations, suggests the possibility of constructing a computer expert system to carry out the analysis automatically. There are several published attempts to construct operability study records, or process fault trees, automatically (see for example 6, 7, 8), but these have not been notably successful, especially when dealing with process flowsheets of any significant complexity.

Generation of cause and symptom equations, or equivalent relationships, from expert rules applied to the P and I diagram structure is the subject of a second package currently under development. Advances in computer-aided design leading to automatic production of P and I diagrams will eventually enable the design engineer to calculate and display the significant fault states that a proposed design could entail. CAFOS is the first contribution to this capability.

FAULT TREE DISPLAY BY CAFOS

Appendix 1, extracted from Reference 3, lists cause and symptom equations from an operability study of an ammmonia let-down system. The first object of the CAFOS program is to convert

these equations into the logical interconnection of events, and to display them as fault trees. To do this the relationships only among events are of interest; the names of events are opaque to CAFOS, which reads the equations from a data file, extracts a list of the named events, and constructs a matrix containing the logical interconnections among events.

The list of events, and the matrix of their connections are sent to disc store and used for all subsequent operations performed by the CAFOS package. Fault tree display, initiated by calling for the highest event or for any named event in the tree, is then simple in principle, requiring a suitable pictorial layout of named events in the relationship determined from the connection matrix. This has been done by computer graphics or by text-mode printing (a more portable but less adaptable operation) in versions of the package.

Appendix 1, Figure A1-2 shows text-mode fault trees produced by the VAX FORTRAN77 version of CAFOS for the ammonia let-down analysis.

PROBABILITY CALCULATIONS

From input probability values of the primary events in an analysis, ie those events that have no causes within the analysis, CAFOS uses the matrix of connections and simple rules of probability to calculate the probability values of all other events.

The calculation is simple in principle, working up the trees of unknown values, and using a linked-list calculating sequence that ensures that the immediately lower events in the tree have already been evaluated before a given event is attempted.

The problems of probability evaluation are two:

The Probability Database

All primary events must be given externally defined probability values. These could be supplied for individual events from a data file, or (tediously) on-line, but the CAFOS approach was to use 'generic sets' of named events whose probabilities were thought to be the same for practical purposes. For example, in a large P and I diagram there will be many control valves each within a different name, and all events 'control valve failed' will have a different name, but their probabilities may be the same. At run-time each primary event can be allotted to a new or an existing generic set in a stored data file. In later runs this generic data file can be searched for named events whose probabilities are needed.

The generic set method does not solve the problem of what numerical values to give to the event probabilties, which must be found by experimental observations and by information exchange among practitioners, but it enables doubtful values to be changed easily so that sensitivity analysis is rapid and convenient.

Repeated or Common-mode Primary Events

When a given primary event occurs more than once in a fault tree the basic calculation method for secondary probabilty values is not valid, since the probability rules for combined events assume the events to be independent. An alternative, conditional probability, calculation should then be made:

$$P(E)=P(E/A)*P(A) + P(E/\bar{A})*P(\bar{A})$$

Where;

P(E) - the true probability of event E
P(E/A) - the probability of E, given that A occurs
P(E/$\bar{A}$) - :: :: of E when A does not occur
P(A) - the probabilty of primary event A

P($\bar{A}$) - The probability that A not occur, = 1-P(A)

This conditional probability calculation can, in principle, be extended for any number of repeated events. Thus for two such events, A and B;

$$P(E) = P(E/A,B)*P(A)*P(B) + P(E/\bar{A},B)*P(\bar{A})*P(B) +$$

$$P(E/A,\bar{B})*P(A)*P(\bar{B}) + P(E/\bar{A},\bar{B})*P(\bar{A})*P(\bar{B})$$

but the number of calculations for a given event increases exponentially with the number of repeated events.

CAFOS, which is designed for rapid on-line probability calculations, offers a hierarchy of strategies for repeated events;

(a) ignore the repeated events,
(b) rank the repeated events and include any number of them, up to 10,
(c) a pattern-recognition strategy,
(d) a minimum tie sets method,

taking progressively longer computing times. Reference 9 discusses these methods in detail. Practical trials, see below, have shown that method (b) appears to be adequate for trees with many repeated events.

EXAMPLE OF USE OF CAFOS

Appendix 1 contains a small demonstration example of the application of CAFOS to an ammonia let-down system. It shows the P and I diagram, cause and symptom equations derived from it, and examples of the resulting CAFOS fault trees.

Appendix 2, outlines a larger scale application to an electrical network and contains calculations of comparative probability values for power loss and voltage dip based on alternative ring and star connections of power lines.

CONCLUSIONS FROM APPLICATIONS OF CAFOS

CAFOS has been installed in several major companies, and has found use in the analysis of small and large operability studies, using local and public probability values. Our provisional conclusions from these applications are:

(1) The display of fault trees is of initial interest when the user first looks at the logic of fault interaction, and checks the input equations, but once he is confident of the fault tree structure the quantitative insight from the probability calculations becomes the main benefit from CAFOS.

(2) The generic set probability data files make calculation fast and easy, and compensate for uncertainty in actual probability values, but reliable probabilities for primary events are the limitation to quantitative fault tree applications.

(3) The rapid heuristic methods for dealing with repeated events appeared to be adequate in the applications studied.

(4) The development of a large computer package like CAFOS benefits greatly from real industrial applications.

REFERENCES

(1) Lihou DA (1980), Computer-aided Operability Studies for Loss Control. 3rd International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Basle, 1980 (v2 p579).

(2) Lihou DA (1981), Operability Studies and Hazard Analysis. In 'Hazard Identification and Control in the Process Industries' Oyez Publishing Ltd, London, 1981 (Ch 7).

(3) Lihou DA (1983), Loss Prevention Bulletin 051, p 19, Institution of Chemical Engineers, London, 1983.

(4) Lee WS et al (1985), 'Fault Tree Analysis, Methods and Application - A Review', *IEEE Transactions on Reliability, Vol R-34 p 194, 1985.*

(5) Lihou DA (1983) "Computer-aided Operability Studies'. Private Communication.

(6) Fussel JB (1973), "A Formal Methodology for Fault Tree Construction", Nuclear Eng and Design vol 53 p 337, 1973.

(7) Lapp SA and Powers GJ (1979), 'Update of Lapp-Powers fault tree synthesis algorithm' IEE Transactions on Reliability, vol R-34 p12, 1979.

(8) Taylor JR and Hollo E (1977) ' Experience with Algorithms for Automatic Failure Analysis'. In Nuclear Systems Reliability Engineering and Risk Assessment, JB Fussel and GR Burdick, eds. SIAM 1977.

(9) Jones MC and Booth SH, ' Hierarchy of Heuristics For Probabilities with Repeated Events'. *To be published, (1986).*

APPENDIX 1

Fault Trees for an Ammonia Let-down System

Figure A1-1 shows a simple single stage ammonia let-down system, in which liquid and vapour ammonia separate in vessel C1, liquid at 18 bar in C1 is let-down to 14 bar in C2 via the control valve LCV1.

Vessel C1 has a level control, and C2 has pressure and level controls, and relief valve RV2.

Reference 3, from which this example is taken, discusses the cause and symptom equations for this system, and improvements to the control of the let-down process. Here we give the resulting equations, to show their form, the coding they employ, and the fault trees produced using Table A1-2 as the input file to CAFOS.

Figure A2-2 shows part of the fault trees for the top event 'RV2(141)' ie, liquid ammonia discharged through the relief valve, as derived from the equations (A), (b) and (c) in the above set. The tree sections are in the print-mode format produced by the FORTRAN77 version of CAFOS.

TABLE A1-1

Cause and Symptom Equation Codes for Ammonia Let-Down

Code Number	Property	Guide Word	Component
1	Flow	No	Ammonia Liquid
2	Temperature	Less	Ammonia Gas
3	Pressure	More	Synthesis Gas
4	Level	As well as	Methane
5	Concentration	Part of	Instrument Air
6	Separate	Reverse	
7	Heat Transfer	Other than	

Equipment Type	Index Number 0	-1	1	Letters Used
Alarm	Failed			(FD) failed to danger (IG) ignored
Controller	No signal	Set low	Set high	
Control loop	Valves closed	Giving less flow	Giving more flow	
Level Switch		Set low or stuck high	Set high or stuck low	(FD) failed to danger (FS) failed safe
Line	Fully blocked	Partly blocked		(BV) blocked valve (RV) restricted valve
Transmitter	No signal	Indicates too low	Indicates too high	
Valve	Closed or blocked	Not open enough	Open too much	

TABLE A1-2

Cause and Symptom Equations for Ammonia Let-down System

NB: Cause equations have the operator "=" separating an event from its cause. Symptom equations have "-" between an event and its consequences. The operator "+" separates alternative causes (OR gates). The operator "*" separates events which occur simultaneously (AND gates).

Vessel C1

C1(41) = LT1(1) +LCL1(1)*LAL1(FD)
LCL1(1) = LIC1(-1)+LVV(1)+V3(1)
C1(42) = LT1(1)+LIC1(-1)+V3(-1)
LAL1(FD) = LSL(1)+LAL1(0)+LAL1(IG)
C1(43) = L2(0)+LT1(-1)+LIC1(1)+L2(BV)
+L2|(RV)*LAH1(FD)
LAH1(FD) = LSH1(1_+LAH1(0)+LAH1(IG)
L1(11) - N2(11)*N5(11)
L1(12) - N2(12)*N5(12)
L1(131) - N2(13)
L1(133) - N2(12)*N5(13)
L2(22) - N2(22)*N2(533)*N5(22)*N5(522)
L123 - N2(23)*N5(23)*N5(532)
L1(32) - N2(523)*N5(32)*N5(532)
L1(532) - N5(532)
C1(41) - N2(143)*N5(12)
C1(43) - N5(141)*N2(12)
L5(33) - N2(522)*N5(522)

Line 2

L2(11) = N2(11)+L2(0)=L2(BV)
L2(BV) = V1(0)+LCV(0)=V2(0)
L2(12) = N2(12)+L2(-1)+L2(RV)
L2(RV) = LCV1(-1)
L2(13) = N2(13)
L2(143) = N2(143)
L2(16) = C1(32)*(LCV1(1)+V3(-1)
L2(22) = N2(22)
L2(23) = N2(23)
L2(533) = N2(533)

Line 5

L5(11) = N5(11)
L5(12) = N5(12)
L5(13) = N5(13)
L5(141) = N5(141)+C1(65)
L5(22) = N5(22)
L5(23) = N5(23)
L5(522) = N5(522)
L5(532) = N5(532)

VESSEL C2

C2(32) = PT3(1)+PIC3(-1)+RV2(1)
(B) C2(33) = N3(141)+L2(143)*FAH(FD) + (PLC3(-1)+PCV3(0)*RV2(0)
FAH3(FD) = FT3(-1)+FAH3(0)+FAH3(IG)
C2(41) = LCL2(1)*LAL2(FD)
(C) C2(43) = LCL2(-1)+LCV2(0)+L4(0)
LCL2(-1) = LT2(-1)+LIC2(1)+LCV1(-1)
LCL2(1) = LT2(1)+LIC2(-1)+LCV2(1)
(A) RV2(141) = C2(33)*C2(43)
LAL2(FD) = LSL2(-1)+LAL2(0)+LAL2(IG)

L2(11) - N3(11)*N4(11)
L2(12) - N3(12)*N4(12)
L2(13) - N3(13)*N4(13)
L2(143) - N3(13)*N3(33)
L2(16) - N3(11)*N3(32)*N4(11)
L2(22) - N3(22)*N4(22)*N4(533)
L2(23) - N4(23)*N3(532)
L2(523) - N3(12)
L2(533) - N3(13)
C2(32) - N3N3(532)*N4(22)
C2(33) - N3(12)*N4(23)*N4(533)
C2(41) - N3(12)*N4(143)
C2(43) - N3(141)
RV2(-1) - N3(12)

Line 4

L4(11) = N4(11)+LCV2((0)+L4(0)
L2(12) = N4(12)+LCV2(-1)
L4(13) = N4(13)
L4(143) = N4(143)
L4(22) = N4(22)
L4(23) = N4(23)
L4(533) = N4(533)

APPENDIX 2

Cafos Applied to an Electrical Supply Network

The electrical supply system was a complex interconnection of generators, power lines and distribution buses, with many loops that required careful analysis to avoid logical errors in the cause and symptom equations.

The analysis used 150 equations relating 380 named events, of which 175 were primary events, including 148 repeated primary events in a highly duplicated structure in which the highest events had over 2800 events below them in the fault tree.

Table A2-1 is a comparison of ring and star connection of the power lines. Relative probabilities of power loss and of voltage dip at each of the 13 buses are given for the two configurations, using bus 5 as the reference in both cases. The results required 2 minutes of terminal time to compute using probability values from the generic data files, and using the 10 most significant events in each configuration. Much slower calculations incorporating 15 and 20 repeated events produced very similar results.

TABLE A2-1

Probability Ratios for Power Loss and Voltage Dip

	RING *****		STAR *****	
BUS	Power Loss	Voltage Dip	Power Loss	Voltage Dip
1	1.18	2.95	0.13	3.00
2	1.25	2.55	0.14	2.60
3	1.25	2.55	0.14	2.60
4	1.11	2.56	0.11	2.61
5	1	1	1	1
6	2.67	2.20	0.81	2.24
7	0.56	1.10	0.43	1.12
8	6.96	2.95	1.10	3.00
9	0.56	1.10	0.39	1.12
10	0.53	1.10	0.39	1.11
11	0.53	1.10	0.39	1.10
12	1.30	2.56	0.68	2.61
13	2.19	1.75	0.85	1.78

Figure A2-1 shows part of a typical fault tree section display, with appended probabilities, from the VAX750 FORTRAN77 version of CAFOS, for a voltage dip on Bus 13. The use of such appended fault trees to trace the important contributors to the top event probability will be evident. In this small tree section the major contributors are the primary events ('BOTTOMEVENTS'):

Gen 1 (Volt Dip) :- a generator voltage dip P = 0.100
Line 8 (Hi Load) :- a high line load P = 0.035.

Figure A1-1

SIMPLIFIED AMMONIA LET-DOWN SYSTEM

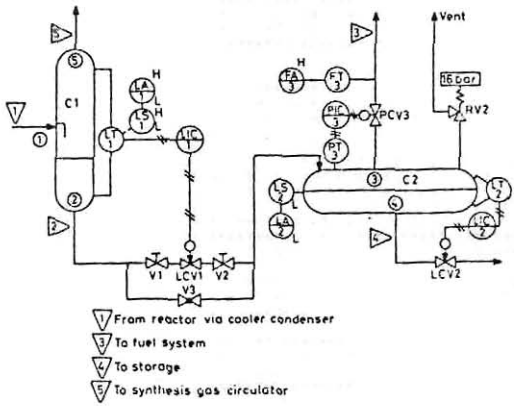


Figure A1-2

FAULT TREE FOR LIQUID AMMONIA RELEIF VALVE RV2

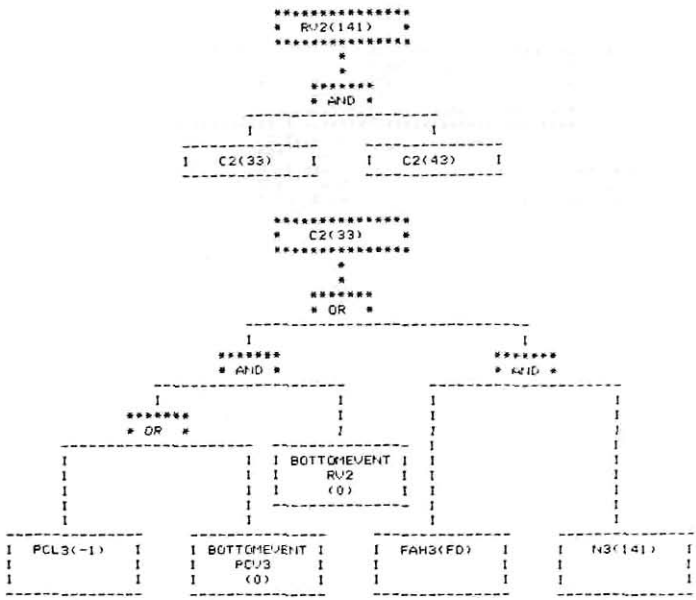


Figure A2-1

FAULT TREE FOR VOLTAGE DIP IN BUS 8