

Comments on the Lapp-Powers 'Computer-Aided Synthesis of Fault Trees'

Howard E. Lambert
TERA Corp, Berkeley

Key Words—Fault tree synthesis, Computer aid, LP algorithm.

Reader Aids—

Purpose: Widen state of the art

Special math needed: Fault tree logic

Results useful to: Reliability analysts, Fault-tree researchers

Abstract—This paper presents a simplified algorithm (than the original Lapp-Powers one) for constructing fault trees for digraphs for negative feedback loops, and describes a) the use of the Lapp-Powers fault tree synthesis algorithm in nuclear material safeguards assessment, and b) the advantages of using digraphs to construct fault trees.

1. SIMPLER LAPP-POWERS ALGORITHM

I believe that the Lapp-Powers (LP) approach would become simpler and more understandable if they change their fault tree synthesis algorithm [1, 2] by —

- 1) Modeling noise in the negative feedback loop operator,
- 2) Dropping use of the exclusive OR(XOR) operator.

The XOR operator is unnecessary from an engineering viewpoint. The XOR operator generates complemented events in the prime implicants that are normally true. A cardinal rule of fault tree construction I learned from David Haasl (DH) [3] is:

“Expect no miracles; those things that normally occur as the result of a fault will occur, and only those thing. Also, normal system operation may be expected to occur when faults occur.”

LP used this DH rule in their algorithm. As an example, if a given disturbance exists which will cause the top event to occur, then LP assume that randomly occurring disturbances of the opposite sign will not cancel the given disturbance.

Using the DH rule, events which reverse gains and in turn cause the top-event variable to deviate oppositely to the specified direction are not considered (because these events are not the result of normal operation). For example, consider event 7 of the fault tree in [2, Fig. 5]. According to the DH rule, event 7 is developed as:

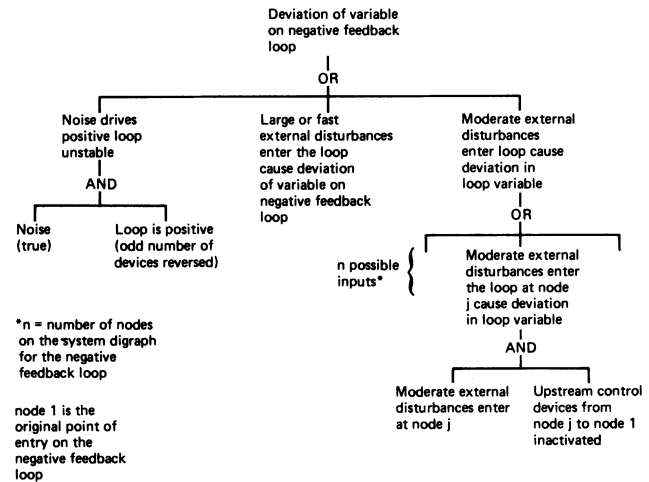
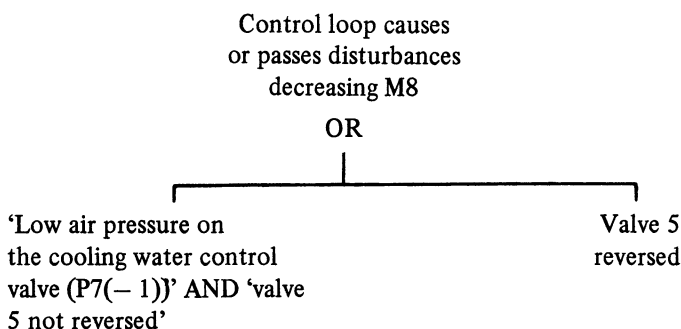


Fig. 1. Simplified NFBL operator.

The event ‘valve 5 not reversed’ is normally true and is deleted when developing the fault tree. In most cases, when one uses DH’s rule, there will be no complemented events in the fault tree and the fault tree is *s*-coherent. When one finds the min cut sets using DH’s rule, some of the min cut sets can be mutually exclusive from a physical viewpoint, i.e., the intersection of two min cut sets might not cause the top event. This is because normally-true conditions are dropped that would make the min cut sets (really the implicants now) mutually exclusive.

When one employs the LP synthesis algorithm using DH’s rule, mutually exclusive events are not generated in the same min cut set due to the consistency checks LP employs for negative feedback loops (NFBLs) and negative feedforward loops.

Fig. 1 gives the simplified NFBL operator for constructing fault trees from digraphs. The important point about this operator is that it considers at once all external disturbances entering the loop. The operator has to be considered only once when developing the fault-tree logic for a deviation of a variable on a NFBL. LP use their NFBL loop operator several times when tracing the cause and effect around the loop. The sign of the external disturbances in fig. 1 is determined by examining the system digraph and establishing the net normal system-gain from the disturbance to the loop variable under development in the fault tree.

The simplified operator gives special attention to the location where moderate disturbances enter the NFBL (see figs. 1 and 2). Moderate disturbances are by definition those which the NFBL is able to cancel. For a moderate disturbance entering a NFBL to cause a deviation of a variable on the NFBL, the following conditions must be met (refer to fig. 2).

1. No control devices are inactivated from the point the disturbance enters the loop downstream to the loop variable

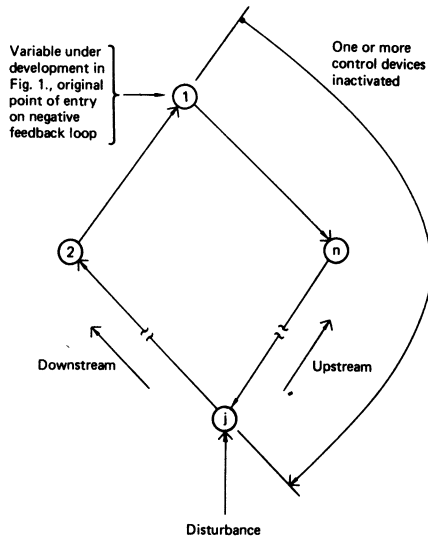


Fig. 2. Failure of NFBL for external disturbance.

under development (the term *downstream* means in the same direction as the arrows are pointing in the digraph).

2. At least one control device is inactivated on the remainder of the loop.

Condition 1 permits the disturbance to propagate down the loop. Condition 2 inactivates the loop so that no corrective action from the NFBL is possible.

In the simplified algorithm, reversal of gains is not considered when external disturbances enter the loop. This is because a reversal event is sufficient to fail the NFBL. In the LP synthesis algorithm, this effect is considered; however the cut sets that are generated by the LP synthesis algorithm are not minimal. When considering how NFBLs can fail when external disturbances enter, (see the two right-hand inputs in fig. 1) the simplified algorithm and the LP synthesis algorithm generate identical min cut sets provided that the use of the XOR operator is dropped in the LP algorithm.

The use of the simplified operator for the event, High Nitric Acid Temperature from Heat Exchanger T3(+ 1) (see system digraph in [2, Fig. 3,]) is given in fig. 3. The identification number for each basic event is shown on the fault tree in fig. 3. There are 19 min cut sets as listed below:

- | | | | | | |
|----|-----|-----|------|-----|------|
| 1. | 3 | 7. | 1,11 | 13. | 2,12 |
| 2. | 10 | 8. | 1,12 | 14. | 2,13 |
| 3. | 14 | 9. | 1,13 | 15. | 2,17 |
| 4. | 15 | 10. | 1,17 | 16. | 4,18 |
| 5. | 16 | 11. | 2,5 | 17. | 6,18 |
| 6. | 1,5 | 12. | 2,11 | 18. | 7,8 |
| | | | | 19. | 7,9 |

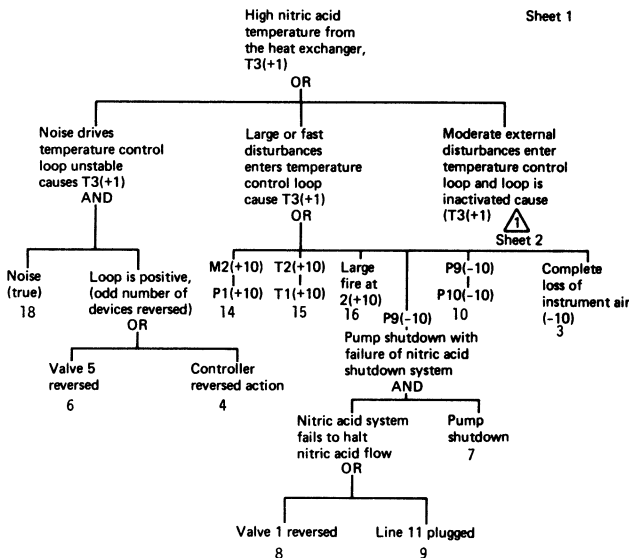
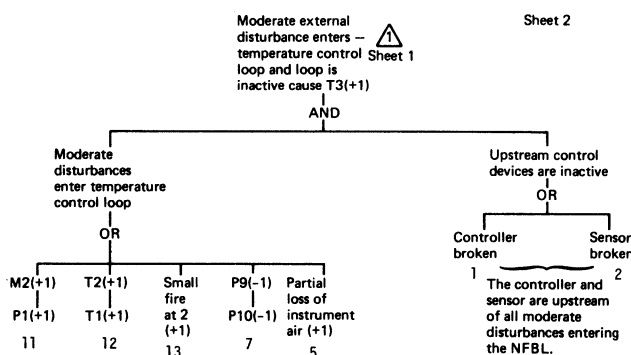


Fig. 3. Fault-tree generated from simplified NFBL operator. (continued below)



Two types of failure were described for control devices on NFBLs [2]:

1. Inactivation of components causing zero gains on the NFBL, eg. controller-broken or sensor-broken.
2. Reversal of components causing a reversal of gains on the NFBL, eg. reversed-valve-action or controller-action-reversed.

There is a third type of failure, not explicitly described in [2], that is modeled as a large input disturbance to the NFBL. This type of failure involves control devices on the NFBL failing high or low and is sufficient to cause a deviation in a loop variable on the NFBL. For example, failures that cause $T_3(+ 1)$ in [2] are:

- 1) valve 5 fails closed,
- 2) controller set point low,
- 3) controller fails low,
- 4) temperature sensor fails low,
- 5) instrument air line rupture.

These failures are modeled as large input disturbances in the simplified NFBL loop operator in fig. 1.

I draw the following conclusions about the simplified operator:

1. When reversal events occur that cause the NFBL loop

to be positive, noise appears as a cause of system failure (eg. see min cut sets 16 and 17).

2. Complemented events (ie. component successes) do not appear in the min cut sets.

3. For external disturbances entering the NFBL, the simplified operator and the LP synthesis algorithm generate the identical min cut sets provided that the use of the XOR operator is dropped in the LP synthesis algorithm.

4. The simplified operator can be used to describe failure of a simple NFBL and cannot be used to describe failure of 1) nested NFBLs or 2) multiple NFBLs affecting the same variable.

5. I found through my experience in teaching fault tree courses that course participants readily understand the rationale behind the logic of the simplified operator. They find it an easy process of searching the NFBL on the digraph and providing the inputs to the fault tree shown in fig. 1. Unfortunately, they found LP's synthesis algorithm for NFBLs much more difficult to comprehend and use.

2. DEMONSTRATION OF THE USE OF LAPP-POWERS FAULT TREE SYNTHESIS ALGORITHM

Lawrence Livermore Laboratory (LLL) is developing an assessment procedure for the U.S. Nuclear Regulatory Commission [4, 5]. The purpose of the procedure is to assess the effectiveness of a potential licensee's material-control system—a system used to protect against theft of special nuclear material (SNM) such as plutonium or uranium 235. An important step in the assessment procedure includes generating adversary sets—the sets of conditions and adversary acts necessary for successful theft of SNM. The study has demonstrated [6] for a complex prototype material-control system that these event sets can be generated from min cut sets of fault trees with top event 'successful diversion of SNM'. These fault trees were systematically obtained from a system digraph by using the LP fault tree synthesis algorithm. The corrective actions of the material control system were modeled by NFBLs and negative feedforward loops. For successful theft of SNM to occur, all the loops on the system digraph must fail.

These loops fail as the result of:

1. Random monitor failure
2. Monitor measurement sensitivity inadequate
3. Human error, including slow guard response
4. Adversary activity, including equipment tampering and collusion.

These 4 events were represented as zero-gain events on the system digraph.

As suggested by Lapp & Powers [7], the loops were found in the system digraph and classified according to their range and dynamics. The corrective action of some loops was so slow, that these loops were failed prior to applying the algorithm. The advantage to this approach is efficiency. One does not need to consider all the combinations of events listed

above that are necessary in failing loops. Hence the resulting fault tree is smaller.

I feel that one major advantage of using digraphs to construct fault trees is the ready display in the system digraph of 1) the cause-and-effect relationships existing between process and state variables and 2) the dynamics of the relationships. In most other techniques, these relationships must be inferred from the system schematic and event descriptions in the fault tree. Hence, I feel that fault trees generated from digraphs give more information than fault trees generated from any other technique. An important aspect of fault tree analysis is the ability to display the analysis to others.

3. ACKNOWLEDGMENT

This report was prepared as an account of work sponsored by the U.S. Nuclear Regulatory Commission under the auspices of the U.S. Department of Energy Contract No. W-7405-ENG-48.

Author Reply

Steven A. Lapp

Design Sciences, Sewickley

Gary J. Powers

Carnegie-Mellon University, Pittsburgh

Dr. Lambert's comments on the XOR are well taken. In most engineering applications, the cut sets one generates using the OR are basically the same as those with the XOR since the complemented events are true with high probabilities. His comments on the consistency checks which prevent mutually exclusive events from appearing in the same cut set are also correct. This section of his paper should help to eliminate some of the confusion which has arisen on this subject.

The part of Dr. Lambert's NFBL operator where he states that 'an odd number of device reversals is necessary to make the loop positive feedback' is exactly the same as our XOR gate. Whether Dr. Lambert's operator is simpler to use must be judged by the reader. Is it easier to recursively-apply our operator around the NFBL or use Dr. Lambert's 'one loop at a time' approach? Again it must be emphasized, as indicated in Dr. Lambert's comments, that his operator will not handle situations where multiple feedback loops pass through the same same variable.

REFERENCES

- [1] G.J. Powers, "Comment on 'Computer-aided Synthesis of Fault Trees'," *IEEE Trans. Reliability*, vol R-26, 1977 Dec, p 316.
- [2] S.A. Lapp, G.J. Powers, "Computer-aided synthesis of fault-trees", *IEEE Trans. Reliability*, vol R-26, 1977 Apr, pp 2-13.
- [3] H.E. Lambert, *System Safety Analysis and Fault Tree Analysis*, Lawrence Livermore Lab., Livermore, Rept. UCID-16237, 1978 May, p 62.*
- [4] "Safeguards Research: Assessing Material Control and Accounting Systems", *Energy and Technology Review*, Lawrence Livermore

Lab, Livermore, Rept. UCRL-52000-77-11/12, 1977 Nov-Dec, pp 11-19.*

- [5] H.E. Lambert, J.J. Lim, *The Modeling of Adversary Action for Safeguards Effectiveness Assessment*, Lawrence Livermore Lab., Livermore, Rept. UCRL-79217, Rev. 1., 1977.
- [6] F.M. Gilman, H.E. Lambert, J.J. Lim, *The Results of a Directed Graph-Fault Tree Assessment of a MCA System*, Lawrence Livermore Lab, Livermore, Rept. UCRL-80802, 1978.*
- [7] S.A. Lapp, G.J. Powers, Engineering short course on "Fault Tree Analysis," Carnegie-Mellon University.

*Available from National Technical Information Service, Springfield, VA. 22151 USA.

AUTHORS

Howard E. Lambert, PhD, PE; Teknekron Energy Resource Analysts Corp; 2150 Shattuck Ave; Berkeley, CA 94704 USA.

Howard E. Lambert has had seven years experience in system safety, reliability and security analysis at Lawrence Livermore Laboratory. He was a fault tree analyst for the Reactor Safety Study. He received the

BS and BE degrees in mathematics and chemical engineering from Youngstown State University, the ME degree in nuclear engineering from the University of Florida, and the PhD degree in nuclear engineering from the University of California at Berkeley. He has worked as a private consultant for Cabot Corporation and the Environmental Protection Agency. He is a lecturer for a fault tree analysis short course given by Stat-A-Matrix Institute at Princeton University. He is with TERA Corporation in Berkeley, California.

Steven A. Lapp; Design Sciences Inc; 407 Edgeworth Lane; Sewickley, PA 15143 USA.

Steven A. Lapp: For biography see vol R-26, 77 Apr, p 13.

Gary J. Powers; Design Sciences Inc; 407 Edgeworth Lane; Sewickley, PA 15143 USA.

Gary J. Powers: For biography see vol R-26, 77 Apr, p 13.

Manuscript TR78-44 received 1978 April 21; revised 1978 October 16.

Author reply received 1979 January 12.

☆☆☆

Manuscripts Received

For information, write to the author at the address listed; do NOT write to the Editor.

"Optimization of maintained systems", Dr. T. Downs; Dept. of Electrical Engineering; University of Queensland; St. Lucia, Qld. 4067; Brisbane AUSTRALIA.

"The sequential destruction method for Monte Carlo estimation of system reliability", M.C. Easton; IBM; PO Box 218; Yorktown Heights, NY 10598 USA.

Correspondence on "A direct method to calculate the frequency and duration of failures for large networks", "Effect of probability distributions on steady-state frequency", Dr. C. Singh; Dept. of Electrical Engineering; Texas A&M University; College Station, TX 77843 USA.

"Ground-hypotheses for the beta distribution as prior in Bayesian estimation", Dr. A.G. Colombo; Commissione delle Comunita' Europee; 21020 Centro Euratom di Ispra (Varese) ITALY.

"Failure rates refined on preventive maintenance and optimum polices", Toshio Nakagawa; Dept. of Mathematics; Meijo University; Nagoya 468 JAPAN.

"A note on maximum likelihood estimation of linear failure rate", Anthony Salvia; Behrend Graduate Center; The Pennsylvania State University; Station Road; Erie, PA 16510 USA.

"A modified block replacement policy using less reliable items", Toshiro Tango; Dept of Clinical Epidemiology; The Tokyo Metropolitan Institute of Medical Science; 3-18-22, Honkomagome, Bunkyo-ku; Tokyo 113 JAPAN.

"An algebraic technique for reliability evaluation", R.K. Tiwari; Dept. of Electronics and Electrical Communication

Engineering; Punjab Engineering College; Chandigarh -160012 INDIA.

"The development of a reliability evaluation program for a new electronic/mechanical watch", Henry A. Buschke; Zenith Radio Corporation; 1000 Milwaukee Avenue; Glenview, IL 60025 USA.

"The informal log-rank versus x test for the exponential distribution: An empirical appraisal and suggestions for use", Dennis W. McLeavey; Dept. of Management Science; College of Business Administration; University of Rhode Island; Kingston, RI 02881 USA.

"Probability plots for life test data based on optimum spacing method", Mr. Masaaki Tsujitani; Dept. of Industrial Engineering; University of Osaka Prefecture; Sakai, Osaka 591 JAPAN.

"Application of the Boolean identity $x_i x_j + x_i \bar{x}_j = x_i$ in the analysis of fault trees", N.K. Nanda; Dept. of Electronics & Communication Engineering; University of Roorkee - 247672 INDIA.

"Availability of coherent structures with several repair units: An application of queueing network theory", Dr. M. Dal Cin; Institut für Informationsverarbeitung; Universität Tübingen; Kßtlinstr. 6; 74 Tübingen WEST GERMANY.

"Analysis of 1-server multi-component system subject to varying rates of repair", "Analysis of 1-server n -unit system", "Expected number of repairs of 1-server 2-unit cold-standby system", Dr. M.N. Gopalan; Dept. of Mathematics; Indian Institute of Technology; Powai, Bombay 400076 INDIA.