System Safety Bookshelf

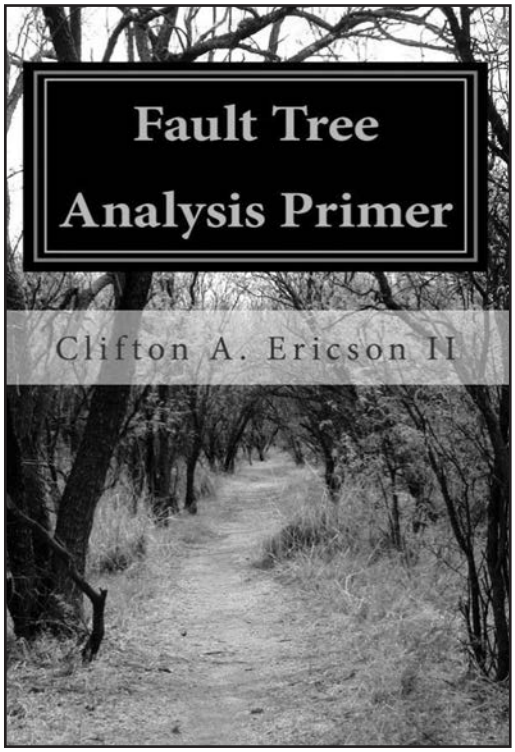
P.L. Clemens, P.E., CSP

A Kind Introduction to FTA

Fault Tree Analysis Primer

By Clifton A. Ericson II
Publisher: CreateSpace
135 pages
ISBN: 10:1466446102
ISBN–13:978–1466446106
Price: $27.00

A color photograph gracing the cover of this book depicts a path winding through a forest of many trees — quite appropriate, given the purpose of the book. It's an inviting path, criss-crossed by shadows that suggest there's a brightly sunlit meadow lying at the path's end. And so there must be! The meadow, in this case, is mastery of a system safety analysis technique that's both reviled and held sacred. But be wary: A clump of brush intrudes into the path. Does a *bête noir* with sharp fangs and a nasty disposition lurk within it? Yes — so stay alert!



Inject the three-word phrase "fault tree analysis" (FTA) into a discussion on any topic among a group of safety professionals. Do it with a flat, unemotional voice. Observe the reactions of others. It doesn't much matter whether fault tree analysis is at all appropriate to the topic under discussion by the group — reactions by your colleagues will be much the same. There will be those who shudder with woe, grimacing and shaking their heads at the mention of FTA. Too often, they make up a majority. But there'll be a few others smiling warmly.

Why do we see these polar opposite reactions? FTA is one of the several system safety analytical techniques that can be applied either subjectively (i.e., non-numerically) or quantitatively. (Couple that with the fact that neither with FTA nor any of the myriad other techniques do we ever actually analyze a system. We analyze only our personal conceptual models of systems — and there, now, is a recipe almost guaranteeing analytical mayhem!) A philosophy that serves in two realms can mistakenly come to be thought of as belonging to neither.

This book opens with an explanation of the function of FTA. Both text and diagrams clarify that identifying hazards is not a principal FTA function. An FTA explores a system to search out those sources and mechanisms that might lead to an already-identified undesirable event. FTA is described as a cause-effect probing of the system. The undesirable event may be a loss event that has, indeed, already occurred — in which case, the FTA then becomes an invaluable investigative tool. A bulleted list of 13 candidates suggests practical applications for which an FTA can be of valuable service. This is but one of this book's many such lists, each speaking silently of having served the author in decades of system safety service and now shared with us to enhance our own practice — each designed to protect against one *bête noir* or another.

This is a kind book, a gentle book. And given the topic, that is a pleasant surprise. Although it commences, as declared by its title, at a "primer" level, it proceeds well into graduate school, taking compassionately small steps as it goes. Its topic is recognized as lying fully across that prickly dividing boundary between the non-numerical system safety methods, i.e., those that might be thought of as almost exclusively "narrative" — e.g., preliminary hazard analysis — and those that are often wholly quantitative, e.g., Markov analysis. This is principally a "teaching" book, and is an excellent choice for classroom use. Nothing more than high school algebra should be needed for its reader to grasp even its most elegant points. And there's stealth and treachery in its di-

dactic methods! You'll read a small handful of paragraphs and discover that you've learned something altogether new to your understanding, or perhaps developed a new outlook toward something you've long understood. And so it is with all of this prolific author's books dealing with topics in system safety.

This book is a badly needed "lite" NUREG-0492, *Fault Tree Handbook* (N. H. Roberts, W. E. Vesely, et al, USNRC, 1981.)

There are valuable hidden lessons that emerge for the user of this book. Here, paraphrased, are two related gems:

- Unquantified fault tree structure alone will reveal much about system risk that might otherwise go undiscovered. A fault tree need not be slathered with statistics to be of value to the system analyst and the system designer.
- If the analyst can't sketch an accurate functional representation of the system, he is not prepared to fault tree it.

Fault tree analysis is not without its limitations and its detractors. Author Clifton Ericson has cataloged a fine "watch-out" chapter that, alone, is worth the price of admission. It is broken into two parts:

- **Common FTA Myths —** Ten myths are presented. Each is followed by a "truth" statement that unarguably sets the record straight. An example myth: If two FTAs for the same loss event and the same system are different in appearance, at least one is incorrect. A pair of differing FTAs is used to explode this myth quite neatly. Their cut sets are identical, but their graphic representations are vastly different from one another, although both of them are correctly drawn.
- **Common FTA Criticisms —** Each of 12 common complaints about FTA by its detractors is presented. A "reality" statement is then presented to correct the disparagement. Partial truths among them are also acknowledged.

And lastly, this book makes an excellent shelf mate to others with titles like these by the same author:

- *Concise Encyclopedia of System Safety*
- *Hazard Analysis Techniques for System Safety*
- *System Safety Primer*
- *Hazard Analysis Primer*
- *System Safety/Reliability Engineering*