

Using Fault Trees to Assess Risk in an Operational Environment

by Richard A. Pullen, Ph.D., Manchester, U.K.
Stephen Flanagan, Ph.D., Manchester, U.K.
John D. Andrews, Ph.D., Loughborough University, U.K.

Abstract

Fault tree analysis is one of the most widely used techniques for probabilistic safety assessments (PSAs). This methodology has traditionally been used to predict the availability of system designs as part of a safety case. However, fault tree analysis can also be used in an operational environment to monitor the effect of failures and scheduled maintenance tasks. The extension of fault tree analysis to operational environments has already been implemented in the nuclear and transportation industries. Great potential exists for extending its use to other industries such as aerospace. Operator aids based on fault tree analysis need not require the end-user to know anything about fault trees or probability theory. Experienced reliability engineers can develop basic fault tree models off-line.

Adapting Fault Trees to an Operational Environment

A fault tree [Figure 1] graphically represents the interaction of failures and other events within a system. Basic events at the bottom of a fault tree are linked via logic symbols (known as gates) to one or more TOP events. These TOP events generally represent system failure modes or hazards for which predicted reliability data is required. Basic events generally represent component failures for which a probability of

failure is given based on historical data. The traditional analysis process is to produce the system minimal cut sets, apply the basic event probabilistic data and then determine the probability of the TOP event.

By using special events known as house events, we can interactively modify the logic of a fault tree to take into account the real-time changes in a system's configuration and status. House events have a probability of one or zero (a true or false status). By switching their status, we can effectively re-configure the fault tree. In addition, component failures may be represented by temporarily converting a basic event to a "true" house event.

Re-analysis of the fault tree, taking into account house event settings, provides the current availability status of the system.

Quantifying Risk Using Event Trees

Event trees may be used to model the consequences of system failures after an initiating event has occurred. Examples of initiating events include *loss of engine*, *fire* and *pipe break*. The likelihood of a consequence is usually expressed as a probability frequency. Each consequence may be assigned a severity according to the consequence category. For example, *probable number of deaths* quantifies the severity arising from a safety conse-

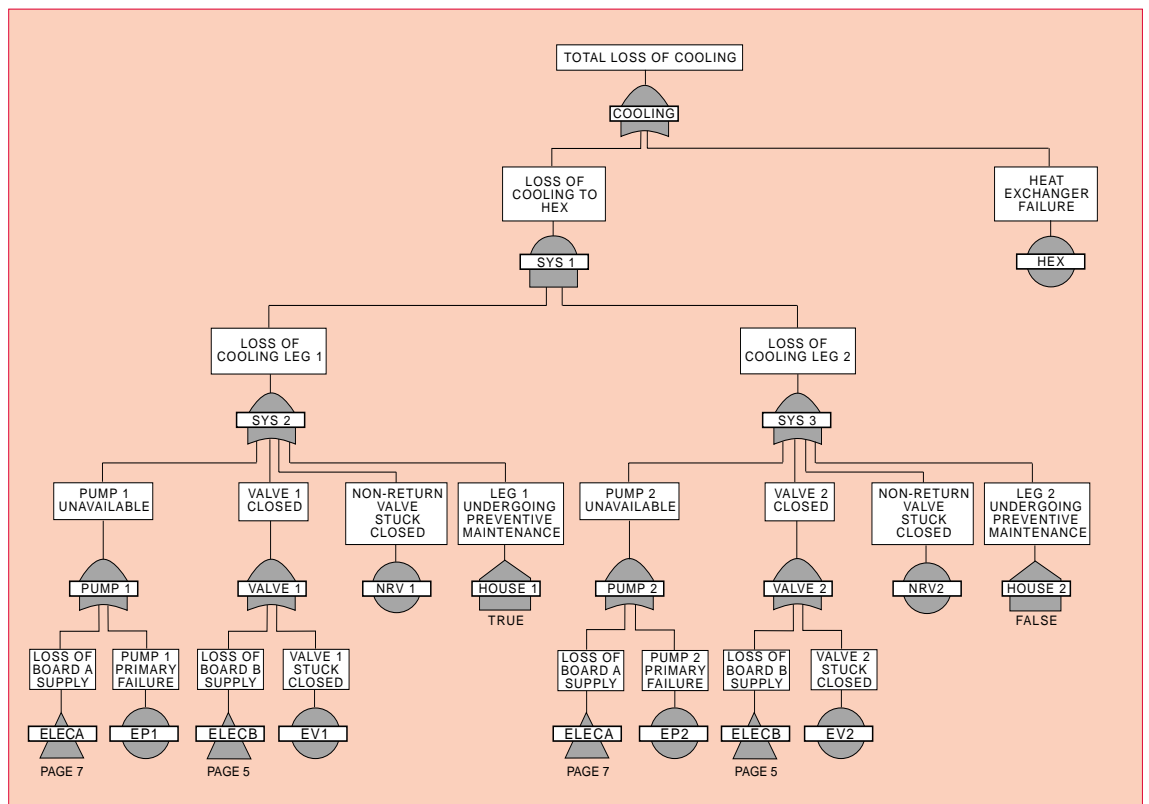


Figure 1 — Fault Tree with House Events Set to Represent Preventive Maintenance Being Undertaken on Leg 1 of the Cooling System.

References for this article are on page 40.

quence. *Likely cost* quantifies the severity of a financial consequence.

Event trees [Figure 2] are often linked to fault trees. We can include event trees in operational PSAs and model the changes in risk due to failures, the effects of scheduled maintenance and other events such as the time of day or system configuration, etc.

Operational PSA tools can answer questions such as:

- Is the plant in a safe condition to continue operating?
- Is it safe to start the mission?
- Can we operate services in the current configuration?
- What are the effects of design changes on safety?
- What is the actual achieved availability history of the plant?
- What are the most likely causes of a system fault?
- How can we optimize the planned maintenance schedule?

Essential Systems Status Monitor

One of the earliest examples of a PSA being performed in an operational environment is the Essential Systems Status Monitor (ESSM) [1]. The ESSM was first installed at Heysham II Nuclear Power Station in the U.K. in 1987. [2]

Documented operating instructions have traditionally been used to stipulate to operators the required levels of redundancy in safety systems. These instructions have to be unambiguous and concise; and due to the complexity of the design of most safety systems, instructions often require a conservative approach.

The ESSM is a computerized tool that uses the same fault tree models and data used in the PSA for the plant. After any change in plant condition (e.g., failure of a component), the ESSM re-assesses the safety status by analyzing the fault trees and taking into account any outages through the use of house events. The system also has the capability to recommend priority maintenance

tasks, again using the underlying fault tree models and house events. System configuration changes are also modeled using house events.

The results of probabilistic assessments are displayed to operators in the form of maintenance categories. These maintenance categories correspond to probability bands. The operators don't see, or need to know anything about, the underlying fault trees.

The ESSM's ability to provide a precise and speedy assessment of the availability status of safety systems allows the station to operate in a less restrictive manner while preserving the same safety objectives. At Heysham II, the essential safety systems include post-trip sequencing equipment, boiler feed systems, essential electrical systems, gas circulators and pressure support systems, etc.

Maintenance planning personnel may also access the ESSM. What-if scenarios can then be examined and maintenance activities planned accordingly.

Exploring What-If Scenarios

Similar procedures can be used as part of a comprehensive management system. Changes in risk can be compared with operational or financial gains by running a program that allows users who are not necessarily familiar with fault tree analysis methods to explore what-if scenarios such as:

- If the level of redundancy in system X is reduced, what are the cost versus risk implications?
- If preventive maintenance intervals are changed, what are the cost versus risk implications?

PSAs in the Rail Industry

Fault and event trees are used extensively in the rail industry to predict the probability frequencies associated with consequences resulting from initiating events such as derailment, fire, etc.

Computer programs that provide a high-level interface for performing PSAs are widely available [3]. They may be used by operators and managers who are not familiar with risk assessment techniques, but who wish to determine the effects of maintenance outages or changes in

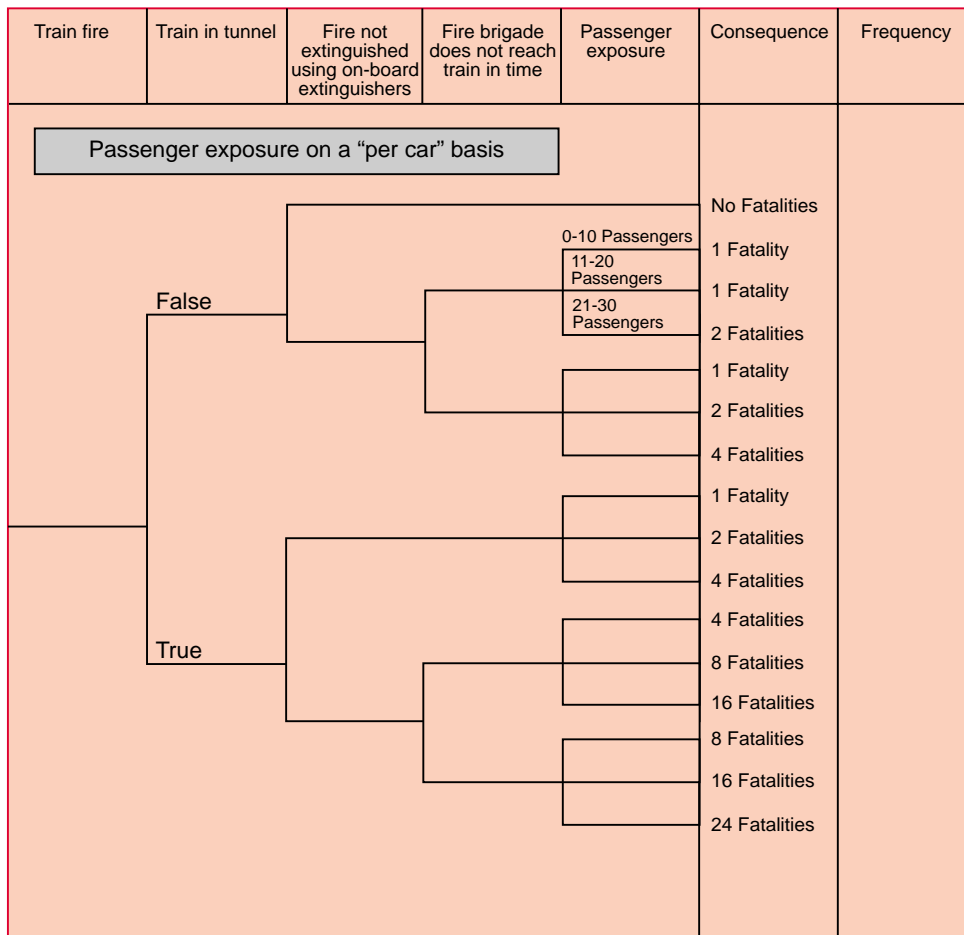


Figure 2 — Example Event Tree from the Railway Industry.

reliability data and event frequencies on the risks associated with a system. These programs allow cost benefits to be weighed against changes in risk [Figure 3].

Such programs are beneficial in analyzing probabilistic risk models that have been created by reliability engineers using similar fault tree analysis programs. The probabilistic risk models contain fault and event tree models that link component failures and other events through sub-system and system failures to consequences for which risks may be quantified. When using any of these interface type programs, the user need not know anything about these fault and event tree models.

By manipulating house events — as with the ESSM system — and modifying basic event probabilistic parameters, the system may be used to perform the following principal functions:

- Vary the reliability of individual components or groups of components, and determine the effect on risk and cost. This function allows a system design to be optimized from a risk and cost viewpoint.
- Determine the effect on risk of current component outages due to maintenance or failure. This is often termed *live probabilistic risk assessment* and enables operators to monitor the current safety status of an operating system.

- Determine the effect on risk of planned maintenance activities. This function allows the scheduling of maintenance activities to minimize risk.

Potential Applications for Operational Risk Assessment

The ESSM system used in conjunction with PSA risk assessment programs offers real examples of how fault trees and event trees may be used in an operational environment to assess the impact on risk of the current status of systems. These programs have been applied principally in the nuclear and rail industries.

There are other industries in which this type of methodology might be employed. For example, computerized tools based on fault tree and house event methodology could also be used to determine whether the probabilistic safety status of an aircraft system is sufficient for take-off.

Summary


Fault tree analysis can be employed effectively in an operational environment to allow systems to operate in a less restrictive and more cost-effective manner. Modern computers allow assessments to be performed quickly, giving precise probabilistic results. These methods also allow planning to consider what-if scenarios. Users of operational

PSA tools such as the ESSM risk assessment programs do not need to be trained in fault tree analysis techniques. The basic fault tree models may be developed off-line by experienced reliability engineers.

About the Authors

Richard A. Pullen, of Isograph, Ltd., obtained his Ph.D. at Imperial College in London in 1981. Since then, he has been involved in the development and application of reliability methods in a wide range of engineering industries. He is the principal author of the FaultTree+ computer program.

Stephen Flanagan, of Isograph, Ltd., obtained his Ph.D. at Manchester University in 1975. Since then he has managed numerous safety-related projects in a wide range of industries.

John D. Andrews is a professor in the Department of Mathematic Sciences at Loughborough University. He has produced numerous journal/conference publications, along with a jointly authored book entitled *Risk and Reliability Assessment*. 

Article References

t Trees to Assess Risk in an Operational Environment (Pages 26-28)

1. "ESSM Gives On-line Real Time Probabilistic Reliability Assessment," *Nuclear Engineering International*, May, 1989.
2. "Employing PRA Techniques in an Operational Environment," *Nuclear Engineering International*, January, 1986.
3. *RiskVu V2 User Manual*, Isograph, 1999.

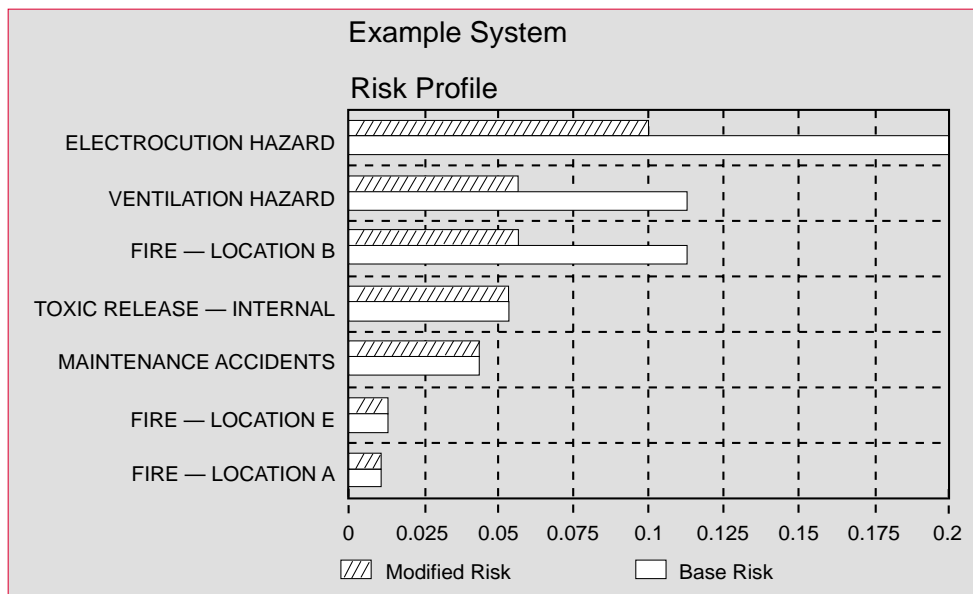


Figure 3 — Risk Profile Comparing "Base" Risk with "Modified" Risk.