



Quantified Risk Assessment Techniques - Part 3

Fault Tree Analysis - FTA

Introduction

Previous Health and Safety Briefings have discussed Failure Modes and Effects Analysis and Event Tree Analysis:

- Risk Assessment Techniques - Part 1 Failure Modes and Effects Analysis - FMEA
- Risk Assessment Techniques - Part 2 Event Tree Analysis - ETA

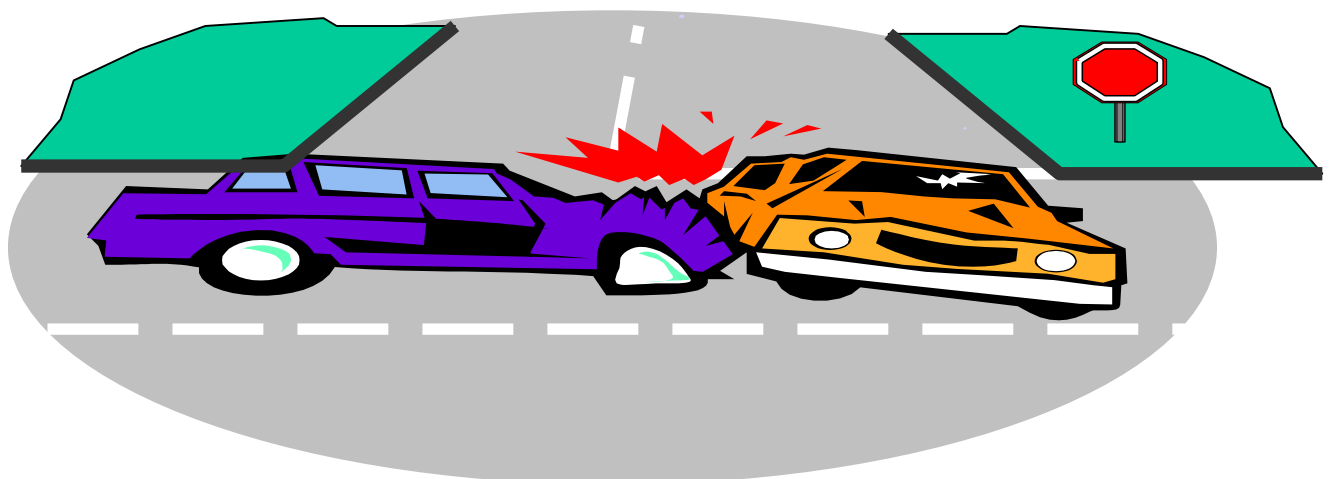
This is the third briefing note to describe a specific risk assessment technique, Fault Tree Analysis - FTA. It must be emphasised that this brief treatment is intended to be illustrative rather than definitive.

Fault Tree Analysis (FTA)

This is a graphical technique that provides a systematic description of the combinations of possible occurrences in a system, which can result in an undesirable outcome. This method can combine hardware failures and human failures.

The most serious outcome such as explosion, toxic release, etc. is selected as the Top Event. A fault tree is then constructed by relating the sequences of events, which individually or in combination, could lead to the Top Event. This may be illustrated by considering the probability of a crash at a road junction and constructing a tree with AND and OR logic gates. The tree is constructed by deducing in turn the preconditions for the top event and then successively for the next levels of events, until the basic causes are identified.

Example: Crash at Main Road Junction



Quantification of FTA

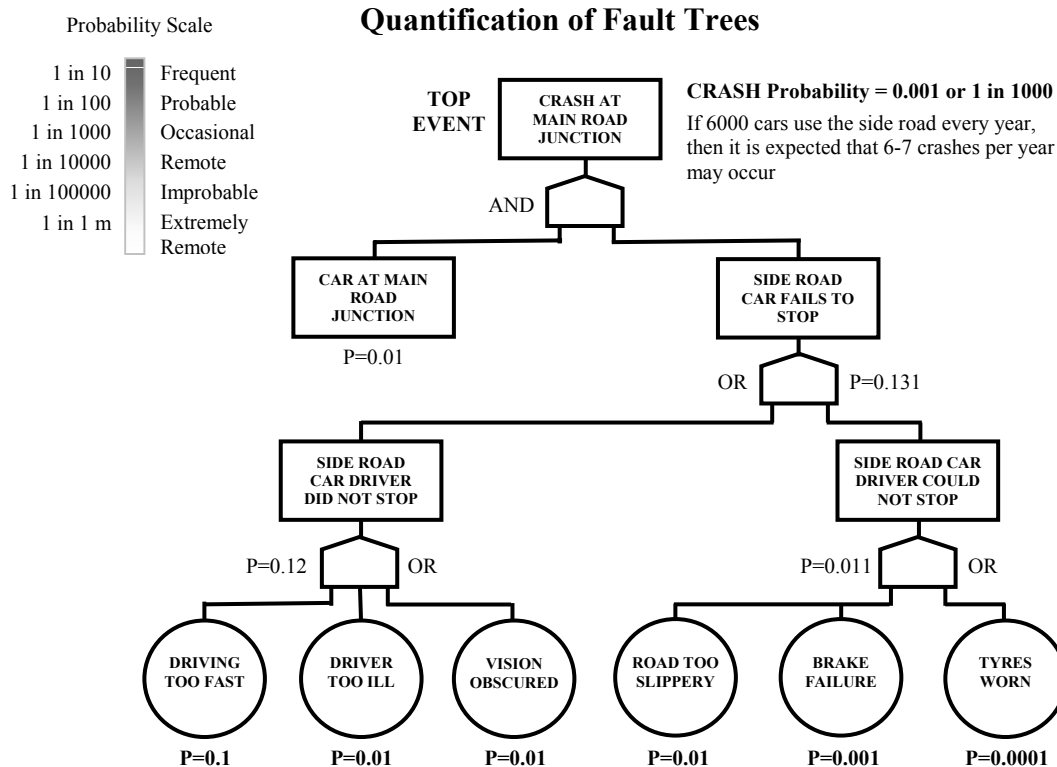


Fig 2

By ascribing probabilities to each event, the probability of a Top Event can be calculated. This requires knowledge of probable failure rates.

At an OR gate the probabilities must be added to give the probability of the next event, whereas at an AND gate, the probabilities are multiplied. This is a powerful technique for identifying the failures that have the greatest influence on bringing about the End Event.

Human Error and FTA

The human error contribution to overall system failure can be included in a Fault Tree Analysis, if human error probabilities are described in the same terms as component and hardware failures.

To include human error, a detailed Task Analysis is first required, breaking down the detail of the actions to be done, taking account of conditions, speed of operation and the correct sequencing of individual actions. Possible deviations can then be identified. After allowing for shaping factors, which influence individual performance, (such as skill, stress etc.), and recovery factors, (most human errors are recoverable), the contribution of human error can be estimated, by using data on human error rates.

References and Further Reading

- Cox & Tait (1991) Reliability, Safety & Risk Management - Butterworth-Heinemann, Oxford
- James Reason (1990) Human Error - Cambridge University Press
- HSE Human Factors in Industrial Safety - ISBN 0 11 885486 0

- IEC 1025 - Procedures and Symbols for FTA
- Risk Assessment Methodologies, H Raafat University of Portsmouth - ISBN 1 069959434

These Briefings contain a summary of recent Health & Safety issues, provided for general information purposes only, and should not be relied upon as legal advice. The IEE has tried to make the Briefings accurate and informative, but they have not been prepared by a lawyer and may not constitute an up-to-date summary of the law. The IEE accepts no liability for your use of these Briefings. Further details and information on broader Health & Safety issues can be obtained from the Government's Health and Safety Executive. Legal advice should be obtained on any specific issues.

The IEE is unable to provide further information on this topic. Please contact the [HSE](#).

For information about the IEE's [Health and Safety Policy Advisory Group](#) please contact:

Health and Safety Policy Advisory Group Secretary
Engineering Policy Department
IEE
Six Hills Way
Stevenage
Herts
SG1 2AY

Tel: +44 (0) 1438 765687