



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY
BY EVERYONE'S SMART UNIVERSITY

Operational & Strategic Risk Management

PMG630

Lecture 6

Prepared by
Dr. Nael Zabel

www.midocean.ae

fault Tree analysis

FTA is a deductive استنتاجي top-down modeling technique used to analyze how a failure can occur. It maps out causal chain of events by connecting hazards and events that can bring about a total or partial system failure. Unlike other risk tools that examine single events or single hazards at a time.

fault Tree analysis

FTA is able to analyze relationships of more than one events together and determine combined effects. Thus, FTA is used extensively in reliability موثوقيه and safety engineering to understand how systems can fail.

WHERE AND WHEN TO USE FTA

FTA is useful in understanding and managing larger and more complex systems. It can be used to show compliance with system safety and reliability requirements or support more robust متين system design. It is useful for developing system or product specifications and for showing critical contributors and pathways to system failure. FTA can extend the analysis of other risk tools such as FMEA, HAZOP, and CCA.

FTA uses graphical methods or diagrams to represent failure events that can occur and show connections that define pathways مسارات to system failure. Failure events in FTA like FMEA are described as risk events. Risk events can be conceived by asking the question What can go wrong?

The top event represents the state of the system taken to be the top risk event. Often it refers to a state of total system failure. Intermediate events represent events that may lead up to the top event. It can refer to subsystem failures or risk events that can cause the top event to occur. Events are denoted by rectangle shapes. Figure 3.7 shows the standard symbols used in FTA.

Standard Symbols in FTA

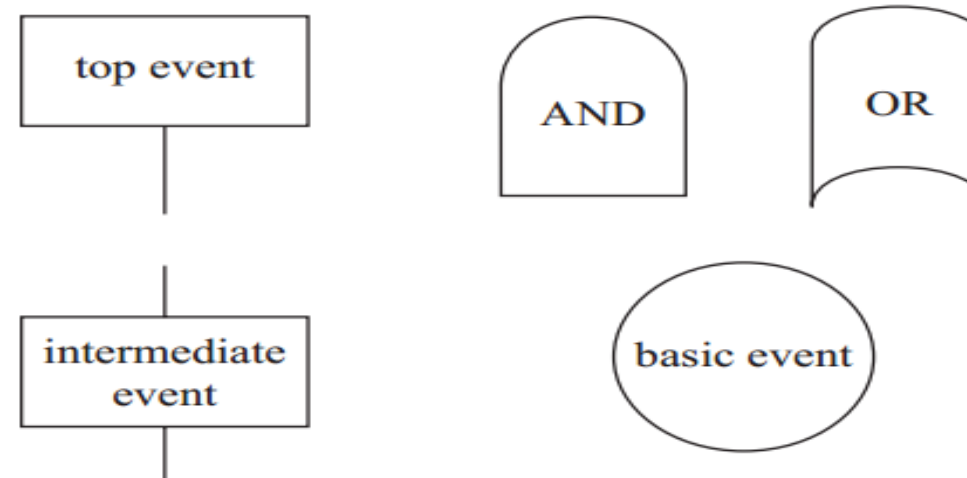


Figure 3.7. Standard symbols used in FTA.

Standard Symbols in FTA

The events interconnect with standard logic gate symbols that represent dependency or contingency relations between events. Thus, two events connected underneath تحت with the logic AND gate are events that are both necessary conditions (both have to happen) to cause the above event to occur.

In contrast, the logic OR gate connecting two events represents two conditions that can cause the above event to occur. In this case, it takes only one of the two events to occur for the top event to happen.

Extending the elevator door example used in the PHA example, sensor failure and mechanism failure are two failure events that contribute to the elevator door closing on an obstruction. The logic diagram is shown in Figure 3.8. As the risk event is caused by any one of these events happening (only one has to occur), the two failure events, both located underneath the logic gate are connected by an OR gate. If either the sensor fails or the mechanism fails or both sensor and mechanism fails, the door will close on the obstruction.

Following the decomposition of the top event to intermediate events, intermediate events are further broken down to sublevels until one reaches the basic events that represent the elementary components (or root causes) that can cause the system to fail. Basic events are denoted by circles.

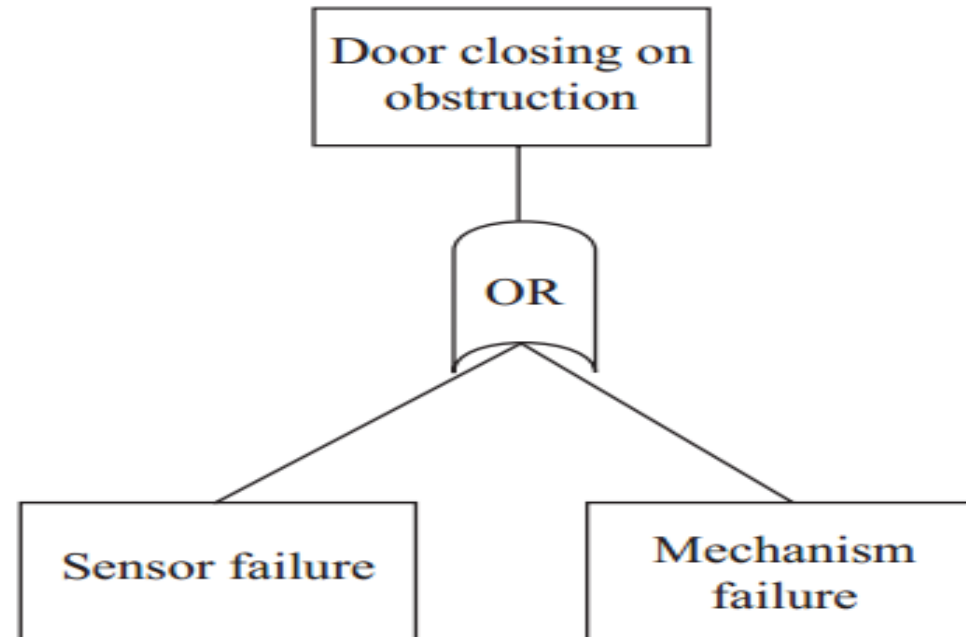


Figure 3.8. Logic diagram for the elevator example.

With the decomposition of events down to the basic events, a tree diagram is formed that outlines the different failure pathways that could cause the top event to occur. Figure 3.9 is an example of a fault tree diagram in FTA. In the traditional solution of fault trees, minimal cut sets can be determined.

Minimal cut sets are all the unique combinations of events that lead up to the top event. Events that are common to these distinct paths should be identified and considered critical. The FTA model can further help in determining which pathways are most likely to occur if data is available on the likelihood of occurrence of the events.

Fault tree construction can be exhaustive, extensive, and time consuming. It is important that one focuses on those events that are regarded as critical and controllable. At times, it may make sense to identify other events that are uncontrollable or not critical and still add them to the model completeness even if they are not further decomposed.

FTA follows a standardized method with rules (i.e., Boolean logic rules). One rule is that there should be no gate-to-gate connections. For example, an OR gate cannot be directly connected to an AND gate. Another rule is that the tree is formed level by level, which means one must exhaustively identify same level events first before constructing the level underneath.

GENERALIZED STEPS FOR FTA

1. Define the system to be analyzed.
2. Describe the top-level risk event (e.g., system failure).
3. Describe intermediate events (e.g., subsystems failure) that contribute to the top-level event and connect them with logic gates as appropriate.
4. Identify sublevel events that contribute to intermediate events and connect same level events with logic gates as appropriate.
5. Repeat (4) until the underlying contributory events الأحداث المساهمة الأساسية are regarded as root causes (basic events).
6. Identify critical events and pathways to failure.

GENERALIZED STEPS FOR FTA

Step 1 begins with defining the system to be analyzed. Consider an FTA of a disabled car. For the succeeding steps, refer to the fault tree diagram in Figure 3.9.

GENERALIZED STEPS FOR FTA

Step 2 describes the top-level risk event. In Figure 3.9, the top-level event of concern is car disabled on the interstate. Specific details such as the location, for example, on the interstate, is significant because a car disabled while in a driveway will have differing analysis. Hence, the conditions surrounding the failure should be described in as much detail as possible.

GENERALIZED STEPS FOR FTA

Step 3 describes the intermediate events that contribute to the top event. Below the top level are the different subsystems failures or risk events that can occur and which are potential causes to why a car is disabled in the interstate.

GENERALIZED STEPS FOR FTA

These risk events are denoted **تدل** as the intermediate events—(1) engine stops and will not start, (2) loss of power, (3) tires out of use, (4) no steering, (5) break failure, or (6) car on fire. If at least one of the intermediate events occurs, it can potentially cause the top-level event to happen. Thus the events are interconnected by an OR gate.

GENERALIZED STEPS FOR FTA

Step 4 describes the next sublevel events that contribute to the intermediate events. After identifying the intermediate events, the events can further be broken down in the next sublevel. Consider the intermediate event tires out of use. Two events have to happen together to cause the car to be disabled on the interstate due to tires out of use—(a) tires lack adequate inflation and (b) spare tire is not available.

GENERALIZED STEPS FOR FTA

Thus the two events are interconnected مترابطه with an AND gate. Note that in the event that the tire lacked adequate inflation but a spare tire is actually available, only one contributory event occurs. Thus, the top event does not occur and the car is not disabled because of the availability of the spare tire.

GENERALIZED STEPS FOR FTA

Step 5 further decomposes sublevel events until underlying contributory event are regarded as root causes, also called basic events. The root causes for the tires lacking adequate inflation are tire blow out from either road or external damager wear and tear. The root causes of spare tire being unavailable are spare tire flavor spare tire missing.

GENERALIZED STEPS FOR FTA

Step 6 identifies the critical events and pathways to failure. Thus, combinations of the basic events identified in step 5 will potentially cause the top event (car disabled on the interstate) to occur from tires out of use. These combinations are listed as follows:

1. Tire blow out from road or external damage and spare tire is flat
2. Tire blow out from road or external damage and spare tire is missing
3. Tire blow out from wear and tear and spare tire is flat
4. Tire blow out from wear and tear and spare tire is missing

GENERALIZED STEPS FOR FTA

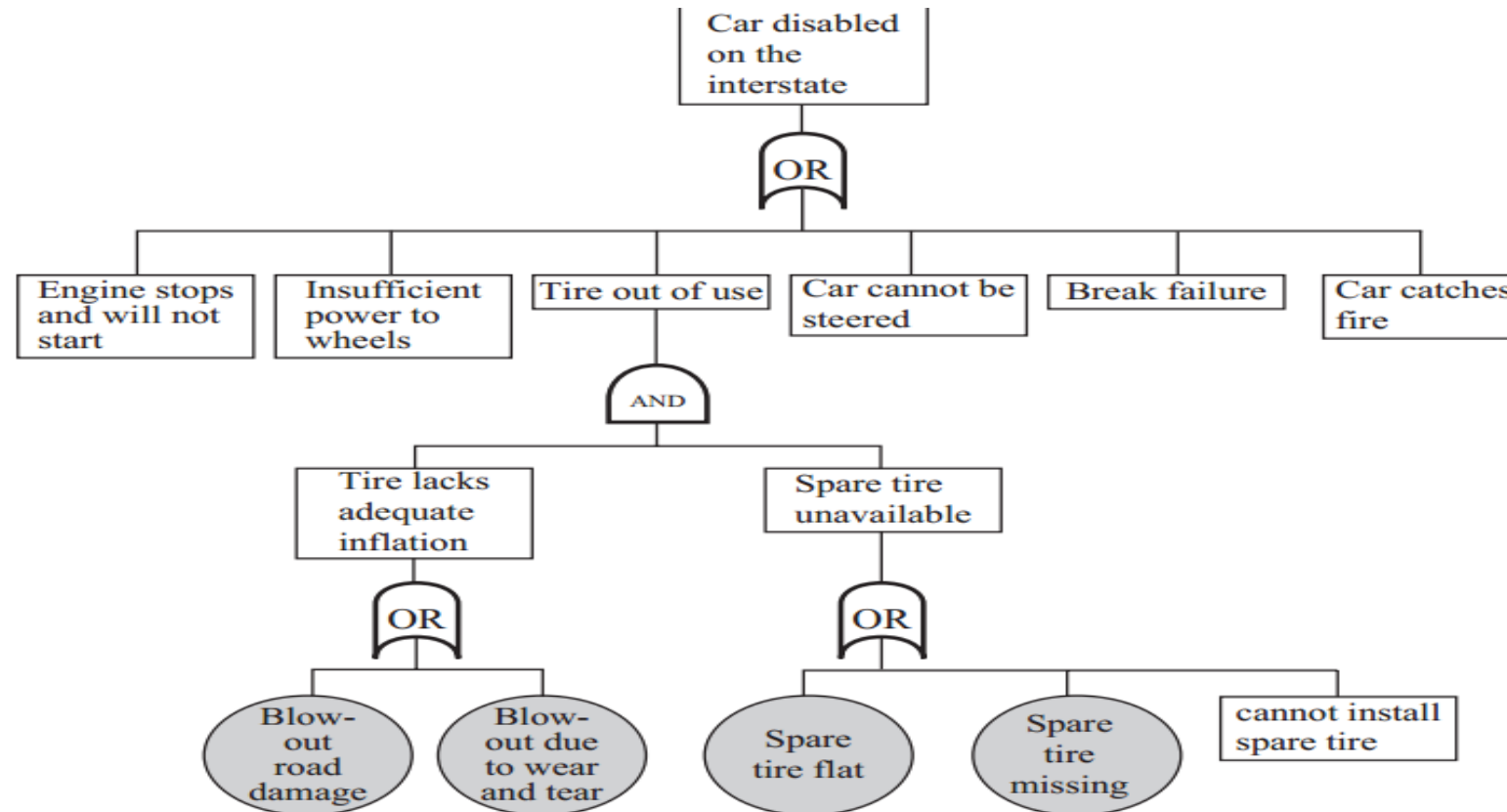


Figure 3.9. FTA for a car disabled on the interstate.¹⁷

cause and consequences

CCA is a modeling **النمذجة** technique that uses graphical methods and diagrams. It is an analytical method for tracing and exposing the chains of events related to a particular risk event of interest. CCA serves as a visual chronological description **الوصف الزمني المرئي** of failures from its initiation to the final outcomes.

WHERE AND WHEN TO USE CCA

CCA is an effective tool for illustrating توضيح the relationships between causes and consequences, especially when examining complex causal event chains سلاسل الأحداث السببية المعقدة where many possible causes and consequences connect to a single event. It is commonly used for analysis of security and safety problems.

WHERE AND WHEN TO USE CCA

It can also be useful for determining requirements for risk management in the design and development of a new system. It can be used for assessing an existing system's performance standards, risk management strategies, and accountability. CCA can be applied as a stand-alone tool in managing risk as well as a support for other tools such as FMEA and HAZOP.

CCA, similar to FTA, uses diagrams to represent failure events and their connections that define pathways to a particular risk event of interest. However, unlike FTA, CCA is organized according to a timeline. The simplest version of a CCA is structured like a bowtie shown in Figure 3.10 where the risk event (the primary event) is positioned in the middle of the bowtie.

The sequence of events that are considered causes is drawn to the left of the bowtie. These events are initiating events that lead up to the primary event. The initiating events can be drawn as an FTA where several levels and sublevels of causality are depicted and where the top event is the primary event. As described in the earlier section, FTA is useful to show how various events may combine to lead up to the primary event.

The sequence of events that are considered consequences is drawn to the right of the bowtie. These events occur as a result of the primary event and are known as the damage chain. Damage chains can be drawn as an event tree analysis (ETA) to enumerate the possible follow-up risk events (consequences) that may arise from the primary event. An example of an ETA is illustrated in Figure 3.11.

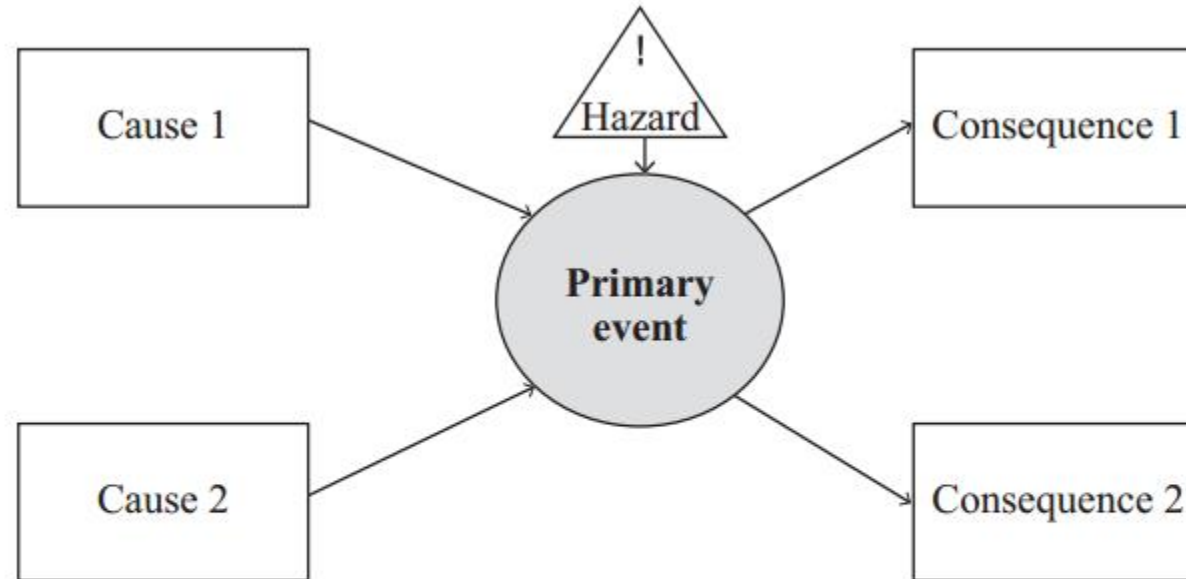


Figure 3.10. Bowtie diagram for CCA.

Event tree analysis

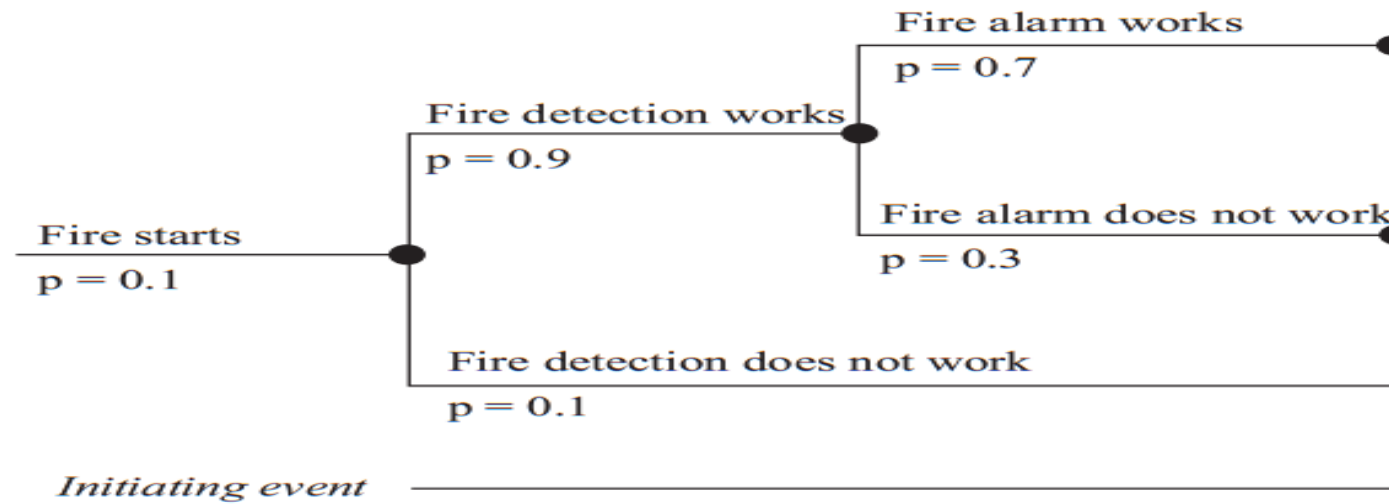


Figure 3.11. Event tree analysis.²¹

Event tree analysis

ETA is a forward logical modeling technique that explores possible consequences or outcomes through a single primary event. The event tree diagram models all possible pathways from the primary event and depicted **يوصف** as branches. Each follow-up event can be intermediate events that in turn initiate other follow-up events.

For example, consider the primary event a fire starts. The follow-up events that are considered are (1) fire detection, (2) fire alarm, and (3) fire sprinkler. For each follow-up event, possible outcomes are enumerated.

For fire detection, two things can possibly happen—the fire detection works or fire detection does not work. Note that in this example, each succeeding event has two possible mutually متبادل exclusive outcomes that can occur. In many cases, there may be more than two outcomes.

CCA can be used fairly directly for quantification of risk and probabilities, but the diagrams can become exhaustive^{شامله} and cumbersome^{مرهقه}. Because of this, CCA is not as widely used as FTA or ETA. Fault and event trees are easier to follow and so tend to be preferred for presentation of the separate parts of the analysis.

Resources:

Operational Risk Management

C. Ariel Pinto

Luna Mylene Magpili

Raed M. Jaradat