RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

Applying Risk Assessement Tools

Chapter 11 — Fault Tree Analysis (FTA)

Chapter Contents

This chapter provides a basic overview of the fault tree analysis technique and includes fundamental step-by-step instructions for using this methodology to analyze a specific accident of interest. Following are the major topics in this chapter:

Summary of Fault Tree Analysis 11-5

Limitations of Fault Tree Analysis 11-9

Procedure for Fault Tree Analysis 11-10

1.0 Define the system of interest 11-12

2.0 Define the TOP event for the analysis 11-14

3.0 Define the treetop structure 11-15

4.0 Explore each branch in successive levels of detail 11-19

5.0 Solve the fault tree for the combinations of events contributing to the TOP event 11-21

6.0 Identify important dependent failure potentials and adjust the model appropriately 11-26

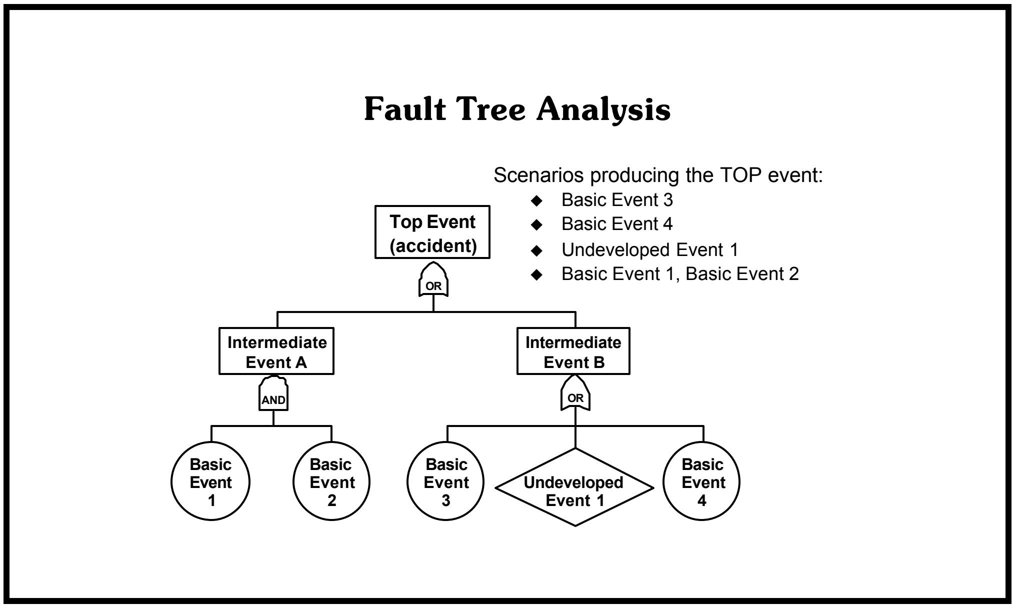
7.0 Perform quantitative analysis (if necessary) 11-28

8.0 Use the results in decision making 11-30

The 5 Whys Technique 11-31

Creating a Simplified Fault Tree for Root Cause Analysis 11-32

See an example of a fault tree analysis in Volume 4 in the Fault Tree Analysis directory under Tool-specific Resources.



Fault Tree Analysis

Scenarios producing the TOP event:

- Basic Event 3
- Basic Event 4
- Undeveloped Event 1
- Basic Event 1, Basic Event 2

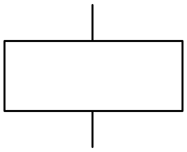
Summary of Fault Tree Analysis

Fault tree analysis (FTA) is an analysis technique that visually models how logical relationships between equipment failures, human errors, and external events can combine to cause specific accidents. The fault tree presented in the figure above illustrates how combinations of equipment failures and human errors can lead to a specific type of accident.

Below is a summary of the graphics most commonly used to construct a fault tree.

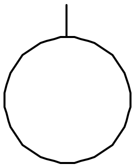
Top event and intermediate events

The rectangle is used to represent the TOP event and any intermediate fault events in a fault tree. The TOP event is the accident that is being analyzed. Intermediate events are system states or occurrences that somehow contribute to the accident.



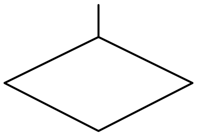
Basic events

The circle is used to represent basic events in a fault tree. It is the lowest level of resolution in the fault tree.



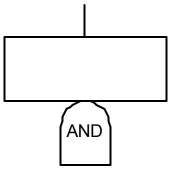
Undeveloped events

The diamond is used to represent human errors and events that are not further developed in the fault tree.



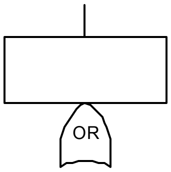
AND gates

The event in the rectangle is the output event of the AND gate below the rectangle. The output event associated with this gate exists only if all of the input events exist simultaneously.



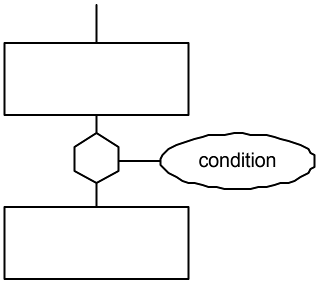
OR gates

The event in the rectangle is the output event of the OR gate below the rectangle. The output event associated with this gate exists if at least one of the input events exists.



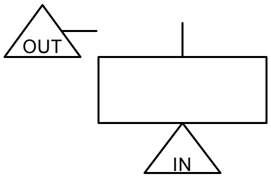
Inhibit gates

The event in the rectangle is the output event of the INHIBIT gate below the rectangle. This gate is a special case of the AND gate. The output event associated with this gate exists only if the input event exists and if the qualifying condition (the inhibiting condition shown in the oval) is satisfied.



Transfer symbols

Transfer symbols are used to indicate that the fault tree continues on a different page.



Brief summary of characteristics

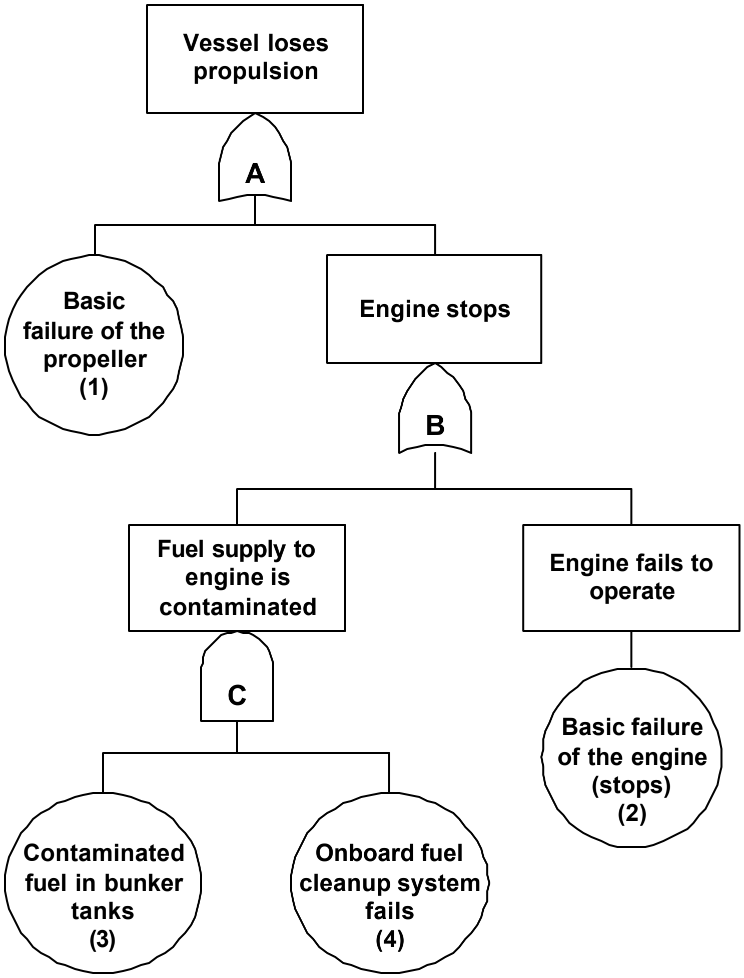
- Models the possible combinations of equipment failures, human errors, and external conditions that can lead to a specific type of accident
- Used most often as a system-level risk assessment technique
- Includes human errors and common-cause failures
- Performed primarily by an individual working with system experts through interviews and field inspections
- A risk assessment technique that generates
  - qualitative descriptions of potential problems and combinations of events causing specific problems of interest
  - quantitative estimates of failure frequencies and likelihoods, and relative importances of various failure sequences and contributing events
  - lists of recommendations for reducing risks
  - quantitative evaluations of recommendation effectiveness

Most common uses

- Generally applicable for almost every type of risk assessment application, but used most effectively to address the fundamental causes of specific accidents dominated by relatively complex combinations of events
- Can be used as an effective root cause analysis tool in several applications
  - to understand the causal factors of an accident
  - to determine the actual root causes of an accident

Example of a predictive application of fault tree analysis

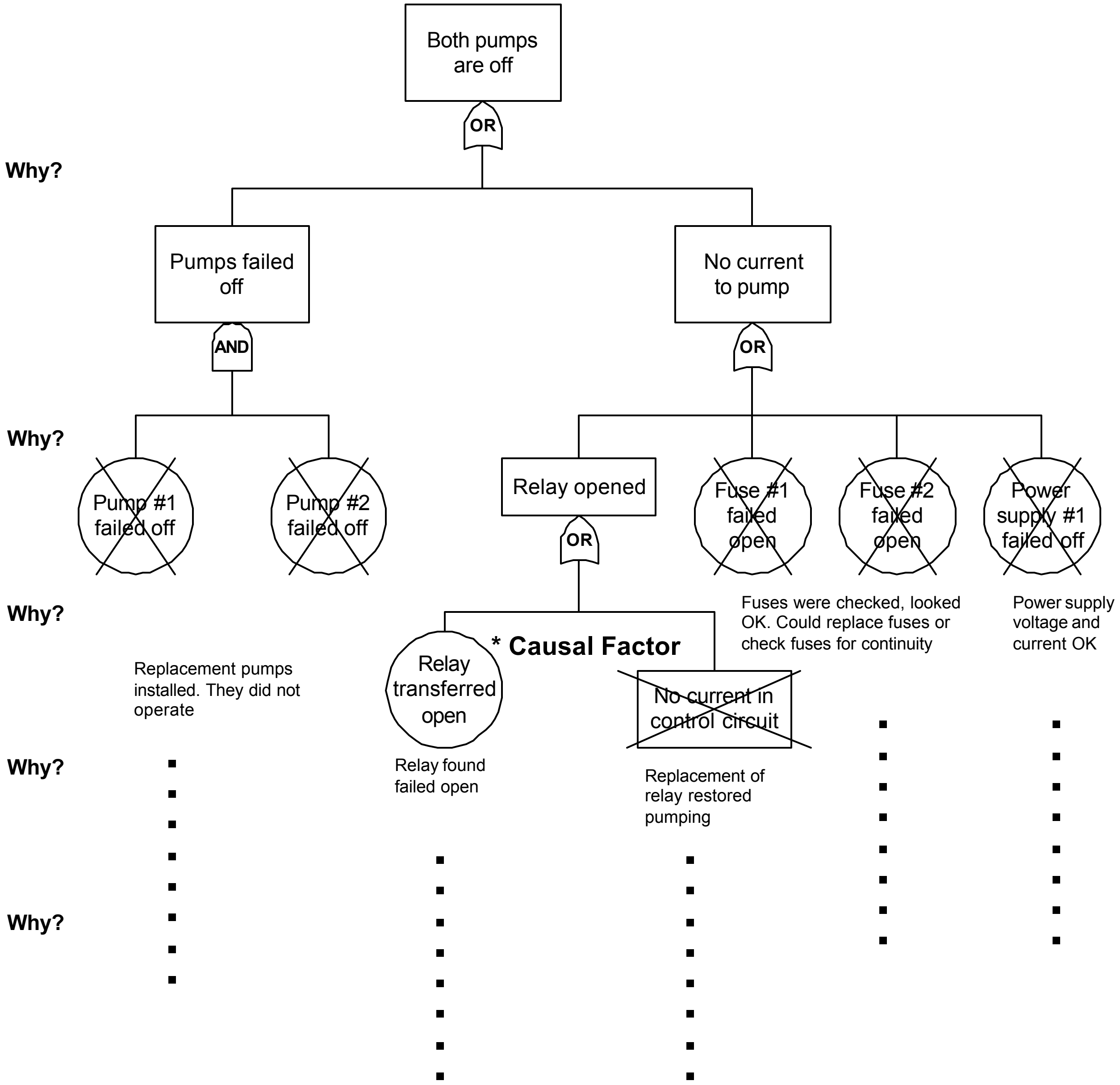
The following fault tree models the combination of events that might cause a particular vessel to lose propulsion. Note that each gate and event is labelled for easy identification and reference. The model would help identify key contributors to the accident of interest so that risk reduction actions could be developed.

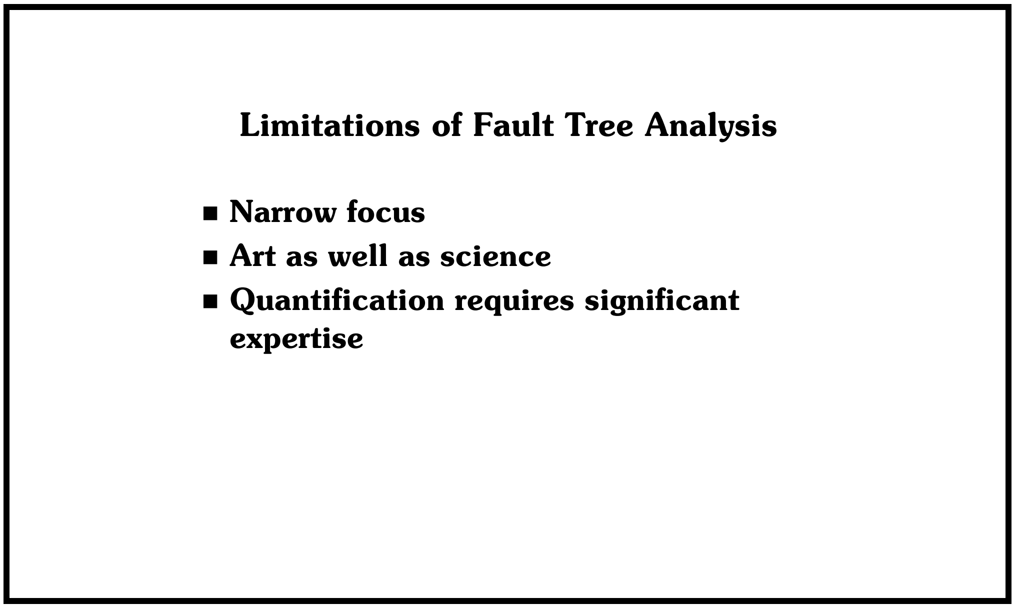

Vessel loses propulsion
A
Basic failure of the propeller (1)
Engine stops
B
Fuel supply to engine is contaminated
Engine fails to operate
C
Basic failure of the engine (stops) (2)
Contaminated fuel in bunker tanks (3)
Onboard fuel cleanup system fails (4)

Example of an investigative application of fault tree analysis

The following is a partial example of fault tree analysis used during an accident investigation. Note that in this case, branches of the fault tree are not developed further if data gathered in the investigation indicate that the branch did not occur. These precluded branches are marked with "X"s in the fault tree, and data are provided to defend the decisions.

Each level of the fault tree is asking "why" questions at deeper and deeper levels until the causal factors of the accident are uncovered.


Both pumps are off
OR
Why?
Pumps failed off
No current to pump
AND
OR
Why?
Pump #1 failed off
Pump #2 failed off
Relay opened
OR
Fuse #1 failed open
Fuse #2 failed open
Power supply #1 failed off
Why?
Fuses were checked, looked OK. Could replace fuses or check fuses for continuity
Power supply voltage and current OK
* Causal Factor
Replacement pumps installed. They did not operate
Relay transferred open
No current in control circuit
Why?
Relay found failed open
Replacement of relay restored pumping
Why?



Limitations of Fault Tree Analysis

- **Narrow focus**
- **Art as well as science**
- **Quantification requires significant expertise**

Limitations of Fault Tree Analysis

Although fault tree analysis is highly effective in determining how combinations of events and failures can cause specific system failures, this technique has three notable limitations:

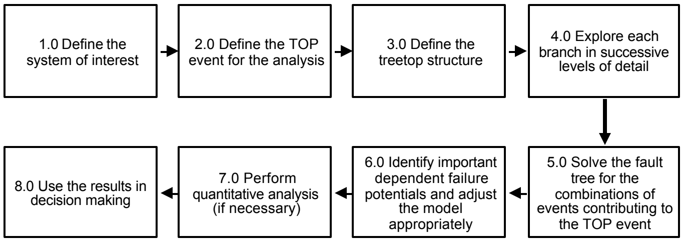
Narrow focus. Fault tree analysis examines only one specific accident of interest. To analyze other types of accidents, other fault trees must be developed.

Art as well as science. The level of detail, types of events included in a fault tree analysis, and organization of the tree vary significantly from analyst to analyst. Assuming two analysts have the same technical knowledge, there will still be notable differences in the fault trees that each would generate for the same situation. However, given the same scope of analysis and limiting assumptions, different analysts should produce comparable, if not identical, results.

Quantification requires significant expertise. Using fault tree analysis results to make statistical predictions about future system performance is complex. Only highly skilled analysts can reliably perform such quantifications.

In addition, analysts often become so focused on equipment and systems that they forget to address human and organizational issues adequately in their models. While this is not an inherent limitation of fault tree analysis, it is worth noting.

Procedure for Fault Tree Analysis


1.0 Define the system of interest
2.0 Define the TOP event for the analysis
3.0 Define the treetop structure
4.0 Explore each branch in successive levels of detail
5.0 Solve the fault tree for the combinations of events contributing to the TOP event
6.0 Identify important dependent failure potentials and adjust the model appropriately
7.0 Perform quantitative analysis (if necessary)
8.0 Use the results in decision making

Procedure for Fault Tree Analysis

The procedure for performing a fault tree analysis consists of the following eight steps:

1.0 Define the system of interest. Specify and clearly define the boundaries and initial conditions of the system for which failure information is needed.

2.0 Define the TOP event for the analysis. Specify the problem of interest that the analysis will address. This may be a specific quality problem, shutdown, safety issue, etc.

3.0 Define the treetop structure. Determine the events and conditions (i.e., intermediate events) that most directly lead to the TOP event.

4.0 Explore each branch in successive levels of detail. Determine the events and conditions that most directly lead to each intermediate event. Repeat the process at each successive level of the tree until the fault tree model is *complete*.

5.0 Solve the fault tree for the combinations of events contributing to the TOP event. Examine the fault tree model to identify all the possible combinations of events and conditions that can cause the TOP event of interest. A combination of events and conditions sufficient and necessary to cause the TOP event is called a *minimal cut set*. For example, a minimal cut set for overpressurizing a tank might have two events: (1) pressure controller fails and (2) relief valve fails.

6.0 Identify important dependent failure potentials and adjust the model appropriately. Study the fault tree model and the list of minimal cut sets to identify potentially important dependencies among events. Dependencies are single occurrences that may cause multiple events or conditions to occur at the same time. This step is qualitative common cause failure analysis.

7.0 Perform quantitative analysis (if necessary). Use statistical characterizations regarding the failure and repair of specific events and conditions in the fault tree model to predict future performance for the system.

8.0 Use the results in decision making. Use results of the analysis to identify the most significant vulnerabilities in the system and to make effective recommendations for reducing the risks associated with those vulnerabilities.

The following pages will explore each of these steps in detail.

1.0 Define the system of interest

- **Intended functions**
- **Physical boundaries**
- **Analytical boundaries**
- **Initial conditions**

1.0 Define the system of interest

Intended functions. Because fault tree analyses focus on ways in which a system can fail to perform a specific function, clearly defining that function is an important first step.

Physical boundaries. Few systems operate in isolation. Most are connected to or interact with other systems. By clearly defining the boundaries of a system, especially boundaries with support systems such as electric power and compressed air, analysts can avoid (1) overlooking key elements of a system at interfaces and (2) penalizing a system by associating other equipment with the subject of the study.

Analytical boundaries. Conceptually, fault tree analyses can include all of the possible events and conditions that can produce a specific type of system problem. However, it is not practical to include all possible contributors. Many analyses define analytical boundaries that do the following:

- Limit the level of analysis resolution. For example, the analyst can decide not to analyze in detail all electrical distribution system problems when studying a vessel steering system
- Explicitly exclude certain types of events and conditions, such as sabotage, from the analysis

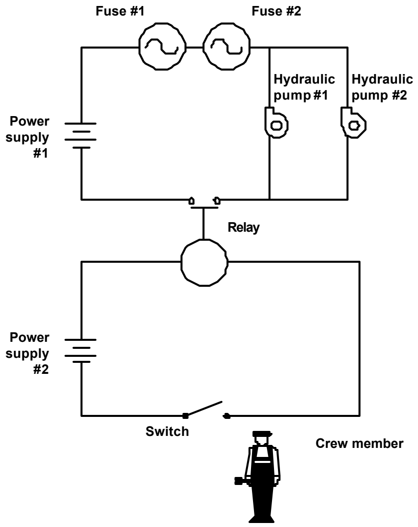
Be very careful about setting analytical boundaries during investigative applications of fault tree analysis. You may be excluding events and conditions that actually contributed to the accident you are investigating.

Initial conditions. The initial state of a system, including equipment that is assumed to be out of service initially, affects the combinations of additional events necessary to produce a specific system problem. For example, if a protective interlock is routinely removed from service, the risk of certain types of problems will be greater. This will affect how the fault tree is drawn and evaluated.

Example

A vessel's hydraulic steering system will fail if both hydraulic pumps fail to operate. The initial conditions and boundaries below were defined before a fault tree was constructed based on the following diagram.

Fault tree results



Function of interest	Boundaries		Initial Conditions
	Physical	Analytical	
■ Provide hydraulic pressure to operate the vessel's steering system	■ Power supply #1 ■ Power supply #2	■ Ignore wiring faults and failures	■ Relay closed ■ Switch closed ■ Pumps on

2.0 Define the TOP event for the analysis

The TOP event must be a specific type of problem with the system

2.0 Define the TOP event for the analysis

Because fault tree analysis is a focused risk assessment tool, begin with a clear statement of the problem of interest. The top event should have the following two elements:

Subject. The entire system or a specific element of the system, such as subsystem, component, etc.

Specific functional failure or condition. A precise description of a problem or condition of interest, defined as narrowly as possible

Poorly defined TOP event (no subject)	Won't start
Poorly defined TOP event (no functional failure or condition)	Motor
Poorly defined TOP event (functional failure not specific enough)	Motor fails
Well-defined TOP event	Motor fails to start

Example

For the scope established in Step 1 (page 11-13), the following is the top event	Both pumps transfer off

3.0 Define the treetop structure

- Logic structure
- Most direct contributors

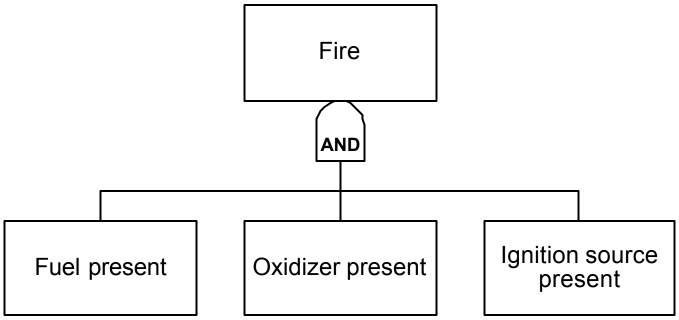
3.0 Define the treetop structure

The next step in a fault tree analysis is to determine the events and conditions (i.e., intermediate events) that most directly lead to the TOP event. This step involves two key elements:

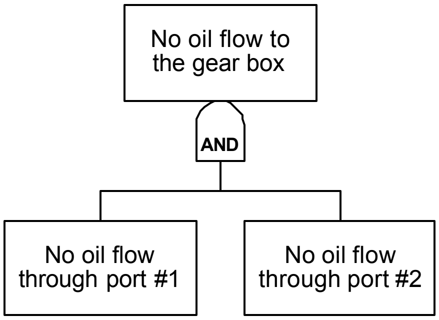
Logic structure. The logical relationship between the TOP event and the underlying contributors

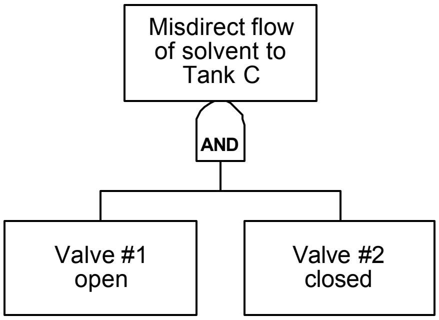
Use an AND gate under the following circumstances:

- Multiple elements must be present for an event to occur or a situation to exist

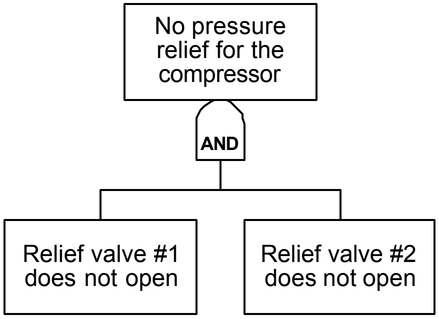


- Multiple pathways (flow, pressure, current, etc.) must all be in specific states (all open, all closed, or some combination) for an event to occur or a situation to exist

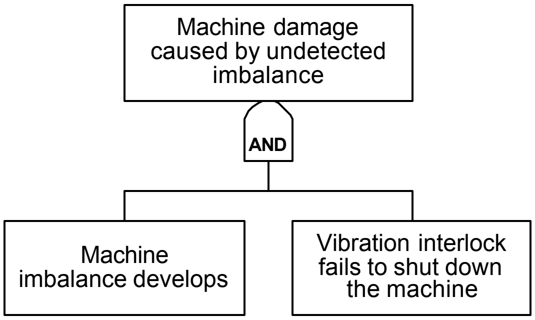

No oil flow to the gear box
AND
No oil flow through port #1
No oil flow through port #2

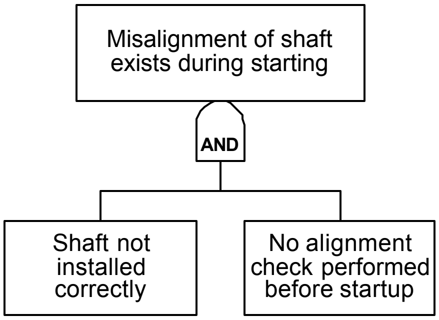


- Redundant equipment items must all fail for an event to occur or a situation to exist


No pressure relief for the compressor
AND
Relief valve #1 does not open
Relief valve #2 does not open

- Safeguards must fail for an event to occur or a situation to exist

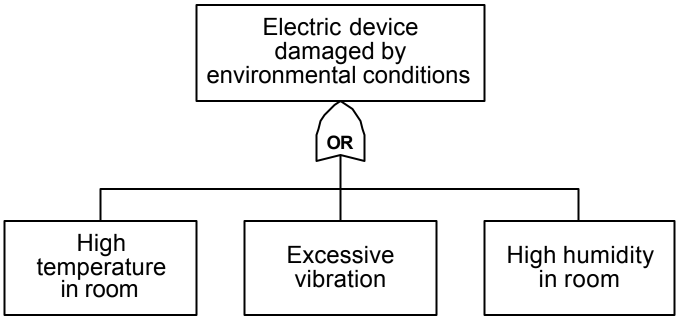

Machine damage caused by undetected imbalance
AND
Machine imbalance develops
Vibration interlock fails to shut down the machine


Misalignment of shaft exists during starting
AND
Shaft not installed correctly
No alignment check performed before startup

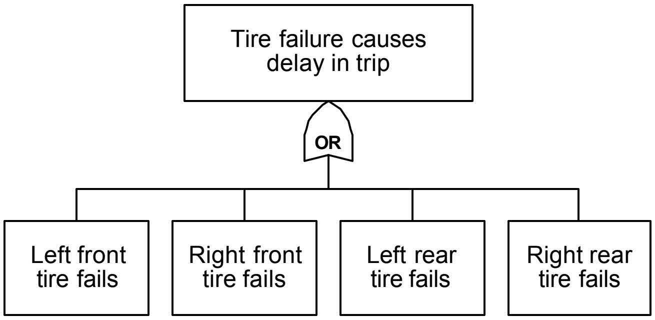
Note: An INHIBIT gate is simply a special form of an AND gate. The INHIBIT gate event occurs when the condition is TRUE ***and*** an input event occurs.

Use an OR gate under the following circumstances:

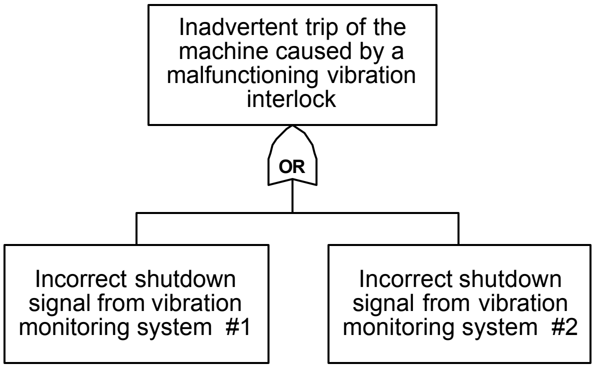
- Any one of several elements can cause an event to occur or a situation to exist



- Failure of any one part of a system causes it to fail



- Any one of several pathways (flow, pressure, current, etc.) in a specific state (open or closed) allows an event to occur or a situation to exist


Inadvertent trip of the machine caused by a malfunctioning vibration interlock
OR
Incorrect shutdown signal from vibration monitoring system #1
Incorrect shutdown signal from vibration monitoring system #2

Most direct contributors. The intermediate events and conditions, generally in broad categories at the upper levels of fault trees, that lead most directly to the TOP event

Like TOP events, intermediate events and conditions should also have the following two elements:

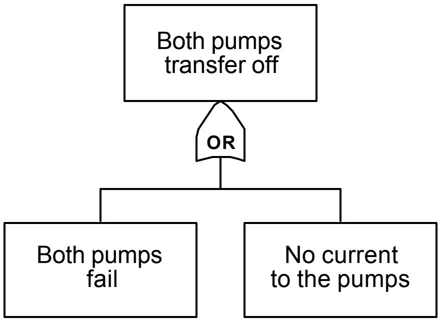
Subject. The entire system or a specific element of the system, such as system, subsystem, component, etc.

Specific functional failure or condition. A precise description of a problem or condition of interest, defined as narrowly as possible

The treetop structure should represent a *baby step* in the analysis of the TOP event. This step of development should take a small, logical step toward the underlying contributors to the problem of interest, but it should avoid the urge to jump to details that are best left to subsequent levels of the tree. By jumping too quickly to the details, analysts often overlook entire branches of development that may be important to the final results. Each level of development should represent the *universe* of possible contributors, excluding those specifically set outside the scope of the study.

Example

For the top event defined in the example in Step 2, the following is an example treetop structure.



4.0 Explore each branch in successive levels of detail

Extend the analysis of each intermediate event to the next level, as if it were a TOP event

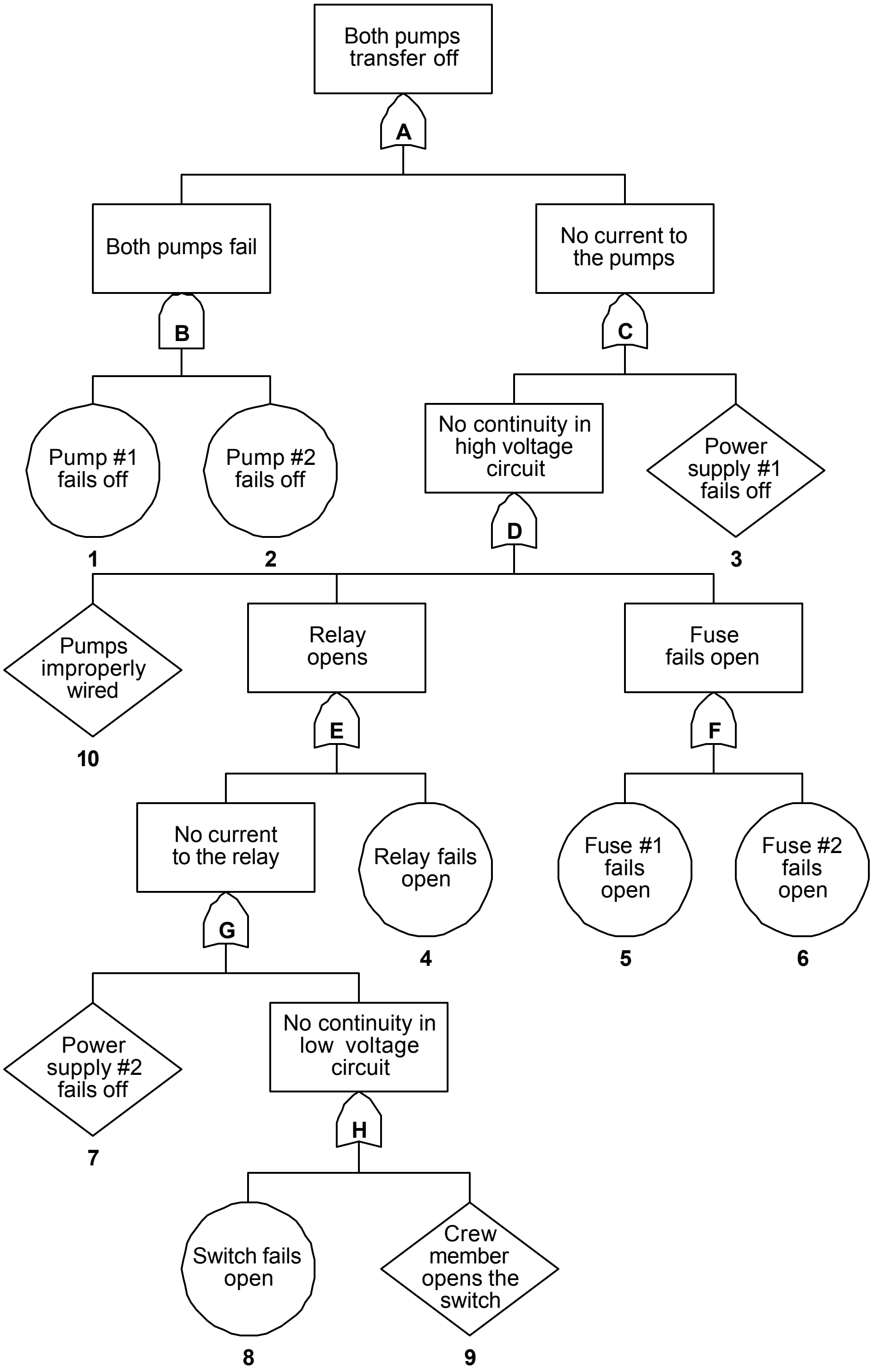
4.0 Explore each branch in successive levels of detail

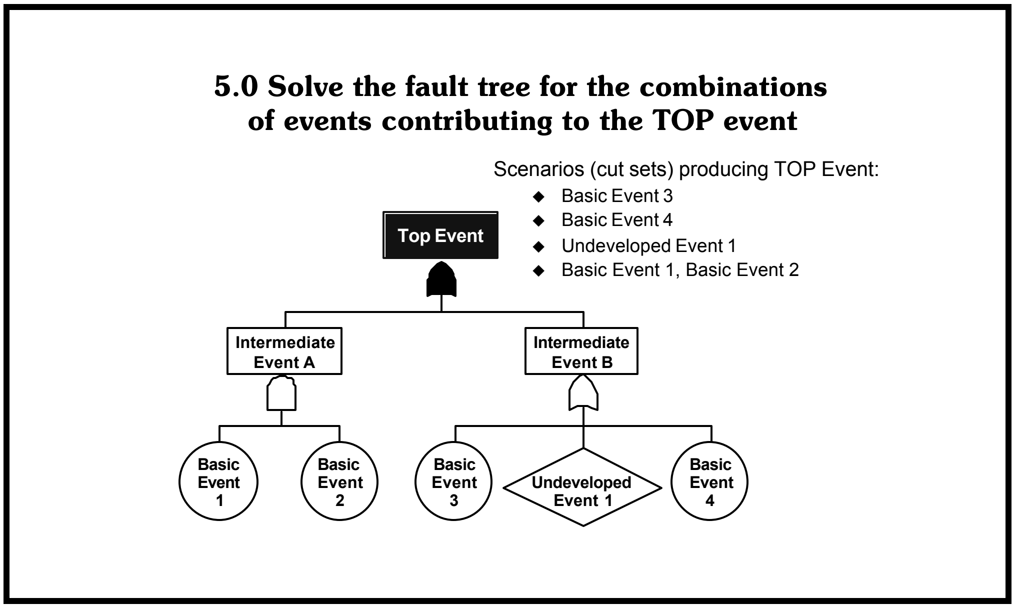
The analysis process continues at successive levels of detail until the model is *complete.* The model is complete when each branch of the fault tree has been pursued to the lowest level of resolution deemed necessary by the analyst. The goal for each branch is to be appropriately descriptive, reasonably exhaustive in the range of possible contributions noted, and exclusive from other branches in the model. Each branch should end with a basic event or an undeveloped event.

By knowing where to stop an analysis, the analysts can avoid overworking problems. There should be just enough detail in an analysis to provide the insights necessary for decision making. It is better to begin with a limited level of analysis and add to it in selected areas than to initially overanalyze the problem.

A good guideline for determining the level at which to stop an analysis is to go no further than those things your organization has control or influence to affect. For example, the configuration of internal circuits in a pressure controller is not typically controlled by the vessel that uses the controller on a system. Thus, fault tree analyses performed for that vessel probably would not go to that level of detail.

Example


Both pumps transfer off
A
Both pumps fail
No current to the pumps
B
C
Pump #1 fails off
1
Pump #2 fails off
2
No continuity in high voltage circuit
D
Power supply #1 fails off
3
Pumps improperly wired
10
Relay opens
E
Fuse fails open
F
No current to the relay
G
Relay fails open
4
Fuse #1 fails open
5
Fuse #2 fails open
6
Power supply #2 fails off
7
No continuity in low voltage circuit
H
Switch fails open
8
Crew member opens the switch
9



5.0 Solve the fault tree for the combinations of events contributing to the TOP event

Scenarios (cut sets) producing TOP Event:

- Basic Event 3
- Basic Event 4
- Undeveloped Event 1
- Basic Event 1, Basic Event 2

5.0 Solve the fault tree for the combinations of events contributing to the TOP event

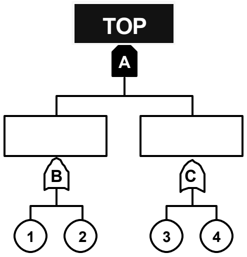
A minimal cut set is a collection of basic events and undeveloped events necessary and sufficient to cause the TOP event. For example, a dead battery and three faulty spark plugs is a *cut set* for the car not starting, but not a minimal cut set. A dead battery alone is a minimal cut set. Three faulty spark plugs alone are another minimal cut set.

For any fault tree, there are generally many minimal cut sets that can cause the TOP event. Some minimal cut sets may be as simple as one event; others may be much more complex, involving 3, 5, 10, or even more events.

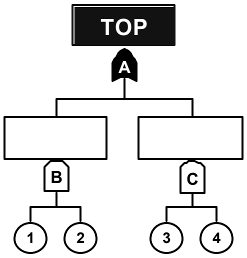
Procedure

5.1 Name all gates, and basic and undeveloped events

Case 1



Case 2

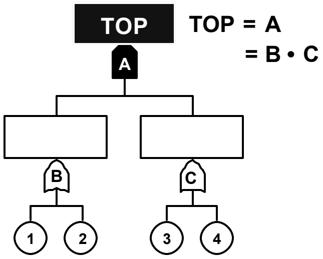


5.2 Beginning with the TOP event, expand each gate into its inputs as follows:

AND Gates: Replace the gate with the product of its inputs

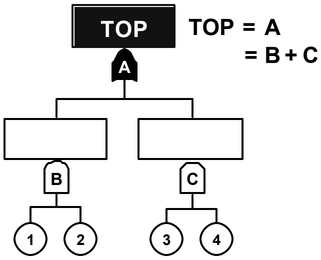
OR Gates: Replace the gate with the sum of its inputs

Case 1 (continued)



TOP = A
= B • C

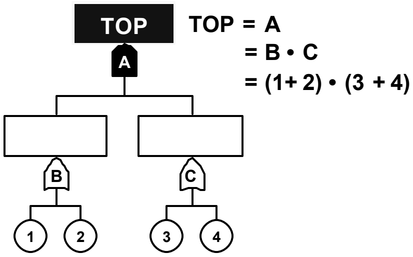
Case 2 (continued)



TOP = A
= B + C

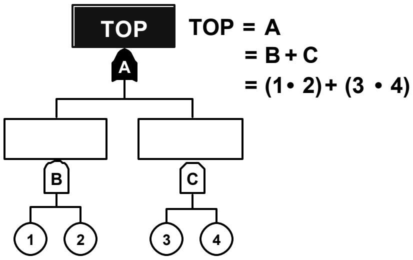
5.3 Continue the expansion until all intermediate event gates have been replaced and only basic events remain in the equation

Case 1 (continued)



TOP = A
= B • C
= (1+ 2) • (3 + 4)

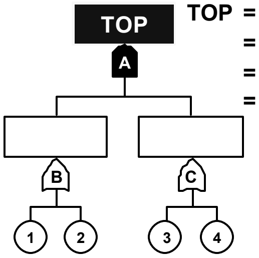
Case 2 (continued)



TOP = A
= B + C
= (1• 2)+ (3 • 4)

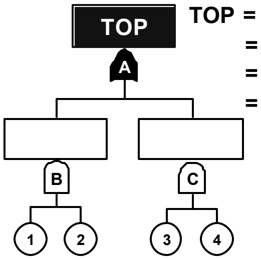
5.4 Simplify the equation by eliminating any parentheses

Case 1 (continued)



TOP = A
= B • C
= (1+ 2) • (3 + 4)
= 1• 3 + 1 • 4 + 2 • 3 + 2 • 4

Case 2 (continued)

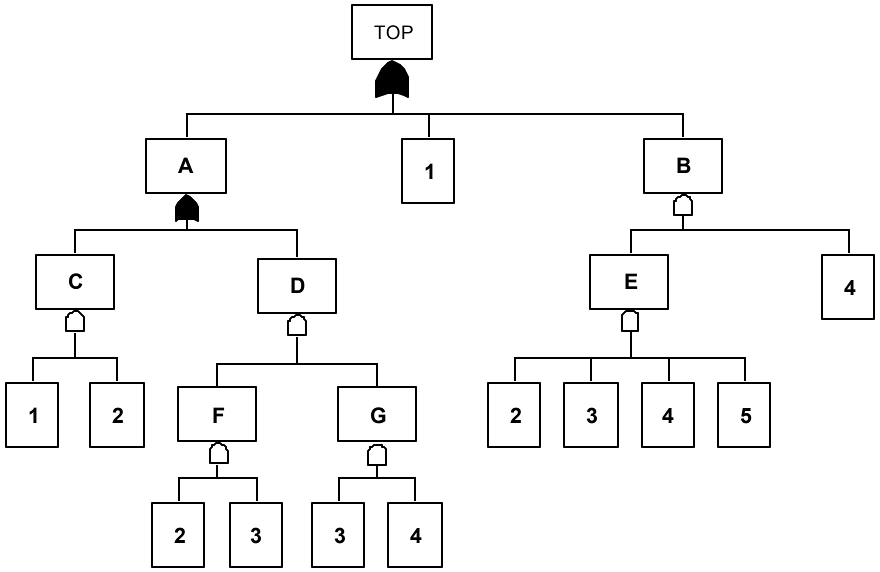


TOP = A
= B + C
= (1• 2)+ (3 • 4)
= 1• 2 + 3 • 4

5.5 Further simplify the equation by:

- Eliminating repeated basic events in cut sets (e.g., the set 1•2•2 becomes 1•2)
- Eliminating supersets, which are cut sets that contain other complete cut sets (e.g., the set 1•2•3 would be eliminated if 1•2 were already a minimal cut set)

5.6 Identify minimal cut sets

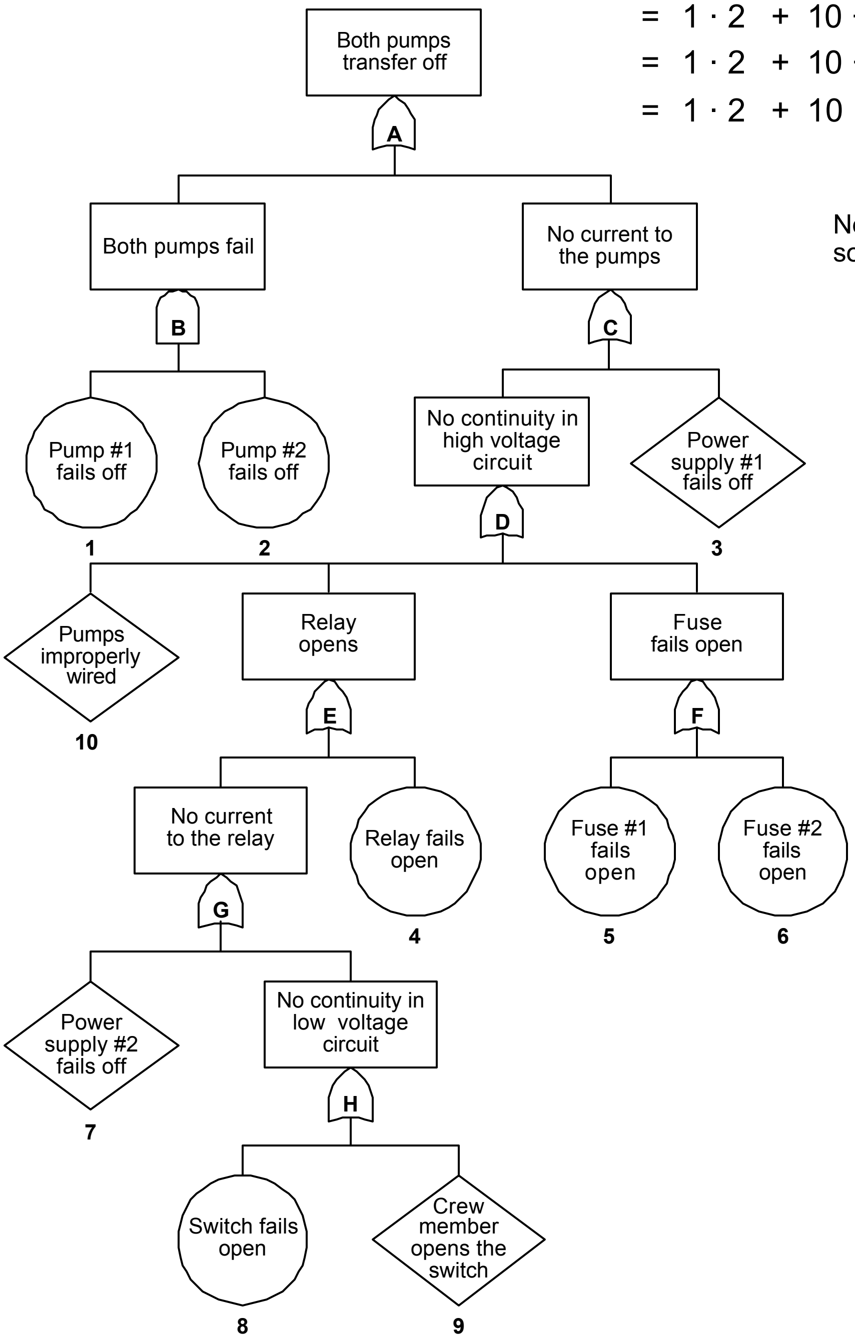


$$
\begin{aligned}
\text{TOP} &= A + 1 + B \\
&= (C + D) + 1 + E \cdot 4 \\
&= 1 \cdot 2 + F \cdot 6 + 1 + 2 \cdot 3 \cdot 4 \cdot 5 \cdot 4 \\
&= 1 \cdot 2 + 2 \cdot 3 \cdot 3 \cdot 4 + 1 + 2 \cdot 3 \cdot 4 \cdot 5 \cdot 4 \\
& \qquad \text{(repeated events)} \\
&= 1 \cdot 2 + 2 \cdot 3 \cdot 3 \cdot 4 + 1 + 2 \cdot 3 \cdot 4 \cdot 5 \cdot 4 \\
&= 1 \cdot 2 + 2 \cdot 3 \cdot \boxed{3} \cdot 4 + 1 + 2 \cdot 3 \cdot 4 \cdot 5 \cdot \boxed{4} \\
&= \boxed{1} \cdot \boxed{2} + 2 \cdot 3 \cdot 4 + 1 + \boxed{2} \cdot \boxed{3} \cdot \boxed{4} \cdot \boxed{5} \\
& \qquad \text{(superset)} \\
&= \underbrace{1 + 2 \cdot 3 \cdot 4}_{\text{Minimal cut sets}}
\end{aligned}
$$

Generally speaking, minimal cut sets with the fewest number of events are more likely, and thus more important, than longer cut sets. Also, events that appear in shorter or more cut sets are generally more important than other events. This type of qualitative judgment about cut set and event importances is called structural importance.

Example

$$
\begin{aligned}
\text{TOP} &= A \\
&= B + C \\
&= (1 \cdot 2) + D + 3 \\
&= 1 \cdot 2 + (10 + E + F) + 3 \\
&= 1 \cdot 2 + 10 + (G + 4) + (5 + 6) + 3 \\
&= 1 \cdot 2 + 10 + (7 + H) + 4 + 5 + 6 + 3 \\
&= 1 \cdot 2 + 10 + 7 + (8 + 9) + 4 + 5 + 6 + 3
\end{aligned}
$$

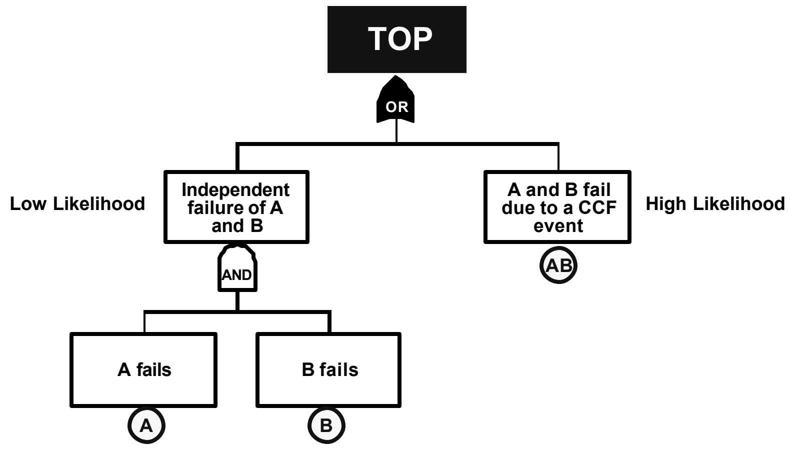


No repeated events or supersets, so the minimal cut sets are:

$$
\left.\begin{matrix} 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{matrix}\right\} \textbf{1-event cut sets}
$$

$$
\left.1,2\right\} \textbf{2-event cut set}
$$

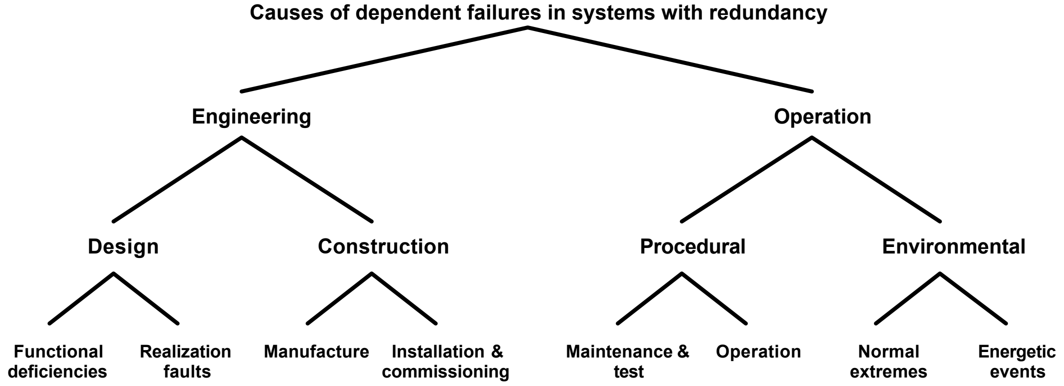
6.0 Identify important dependent failure potentials and adjust the model appropriately


TOP
OR
Low Likelihood
Independent failure of A and B
AND
A and B fail due to a CCF event
High Likelihood
AB
A fails
B fails
A
B

6.0 Identify important dependent failure potentials and adjust the model appropriately

To identify dependent failures, the analyst looks at event sequences for ways in which multiple failures can stem from the same root causes. These common cause failures can defeat several layers of protection at the same time and can, therefore, defeat the redundancy designed into systems. The following figure illustrates some causes of dependent failures that defeat redundancy and layers of protection in systems.

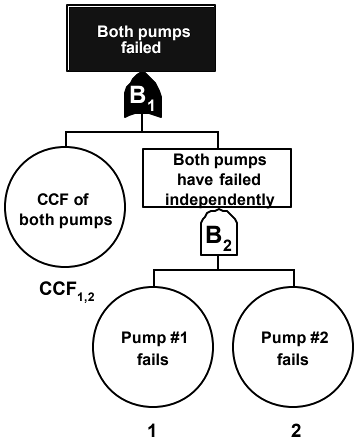
Causes of dependent failures in systems with redundancy



Whenever significant dependent failures are detected, the fault tree model can be modified to include the common cause failure explicitly. Alternatively, the minimal cut sets that contain events with dependencies can be repeated, with the separate independent events replaced by a single common cause event.

Example

The hydraulic pump fault tree example used throughout this section has redundant pumps, which might be vulnerable to common cause failures. The following illustrates how (1) that branch of the fault tree could be revised to account for the common cause failure (CCF) potential and (2) the cut set listing changes with the addition of the CCF event.



Cut Sets

3

4

5

6

7

8

9

10

New cut set **$CCF_{1,2}$**

1,2

7.0 Perform quantitative analysis (if necessary)

- **Characterization of failure mode frequency**
- **Characterization of failure mode severity**
- **Characterization of failure mode risks**

7.0 Perform quantitative analysis (if necessary)

Quantifying the risks associated with potential combinations of human errors and component failures provides more precise results than qualitative analysis alone. Quantifying the risks of potential failure combinations has many benefits:

1. Overall levels of risk can be judged against risk acceptance guidelines, if such guidelines exist
2. Risk-based prioritization of potential failure combinations provides a highly cost-effective way to allocate resources to best manage the most significant risks
3. Risk reductions can be estimated to help justify the costs of recommendations generated during the analysis

There is a wide range of approaches for quantifying the risks of potential system failure modes. These range from very simple binning approaches to more complicated point estimates of frequency and consequence. Volume 2, Chapter 2 provides examples of some of these approaches.

Quantitative analysis of fault trees can be quite complex and requires formal training. The following is only a simple example to illustrate the concept. If you believe your application needs quantitative fault tree analysis, you should get advice and assistance from G-MSE.

Example

For the cut sets identified previously, the following data were gathered.

Event	Rate of Occurrence (λ)	
1	0.1/y	Avg. downtime (τ) = 1hr
2	0.1/y	Avg. downtime (τ) = 1hr
3	1/y	
4	0.01/y	
5	0.001/y	
6	0.001/y	
7	1/y	
8	0.1/y	
9	1/y	
10	0.001/y	
$CCF_{1,2}$	0.01/y	

Based on this data, the overall rate of occurrence for the top event is estimated as follows:

Cut Set	Calculation Process	Values of Cut Set Rate of Occurrence
3	λ_3	1/y
4	λ_4	0.01/y
5	λ_5	0.001/y
6	λ_6	0.001/y
7	λ_7	1/y
8	λ_8	0.1/y
9	λ_9	1/y
10	λ_{10}	0.001/y
$CCF_{1,2}$	λ_1*$CCF_{1,2}$	0.01/y
1,2	$\lambda_1(\lambda_2\tau_2)+\lambda_2(\lambda_1\tau_1)$	(0.1/y)(0.1/y*[1hr*1y/8,760hr])+ (0.1/y)(0.1/y*[1hr* 1y/8,760hr]) = $2.3\text{x}10^{-6}$/y

$$\begin{array}{c}\text{TOP Event}\\ \text{Rate of}\\ \text{Occurrence}\end{array} \approx \sum \begin{array}{c}\text{Cut Set Rate}\\ \text{of Occurrence}\end{array} \approx 3.1/\text{y}$$

8.0 Use the results in decision making

- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**

8.0 Use the results in decision making

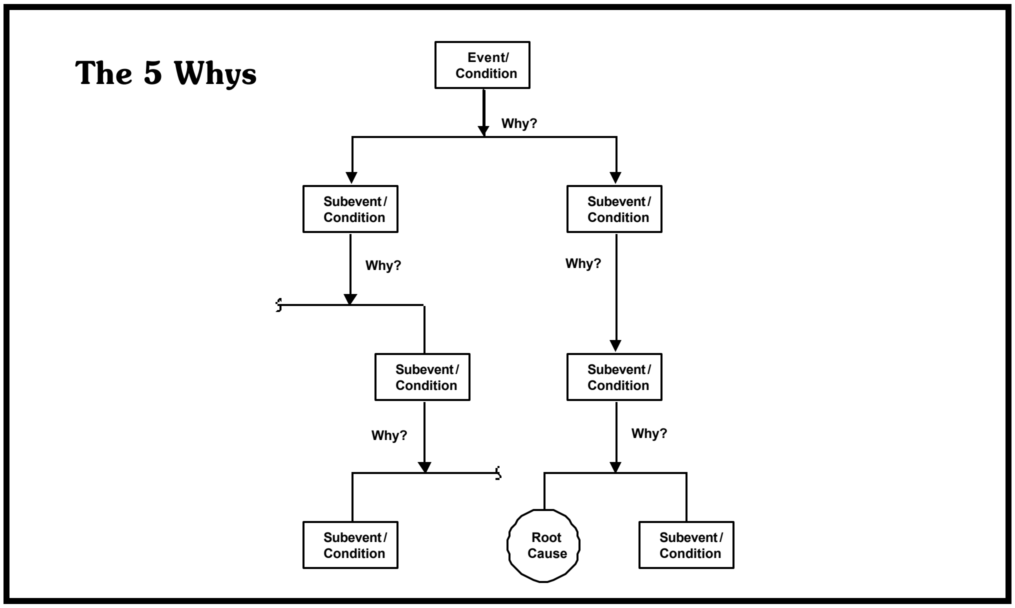
Judge acceptability. Decide whether the estimated performance for the system meets an established goal or requirement. This is generally possible only if quantitative analysis is performed.

Identify improvement opportunities. Identify elements of the system most likely to contribute to future problems. These are the most important events.

Make recommendations for improvements. Develop specific suggestions for improving future system performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes such as planned maintenance tasks, personnel training, etc.

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations will affect future performance. Compare the benefits of these improvements to the total life-cycle costs of implementing each recommendation. This is generally possible only if quantitative analysis is performed.



The 5 Whys

The 5 Whys Technique

The 5 Whys technique is a simpler form of fault tree analysis for investigations, especially investigations of specific accidents as opposed to chronic problems.

The 5 Whys technique is a brainstorming technique that identifies root causes of accidents by asking *why* events occurred or conditions existed.

The 5 Whys process involves selecting one event associated with an accident and asking why this event occurred. This produces the most direct cause of the event. For each of these subevents or causes, ask why it occurred. Repeat the process for the other events associated with the accident.

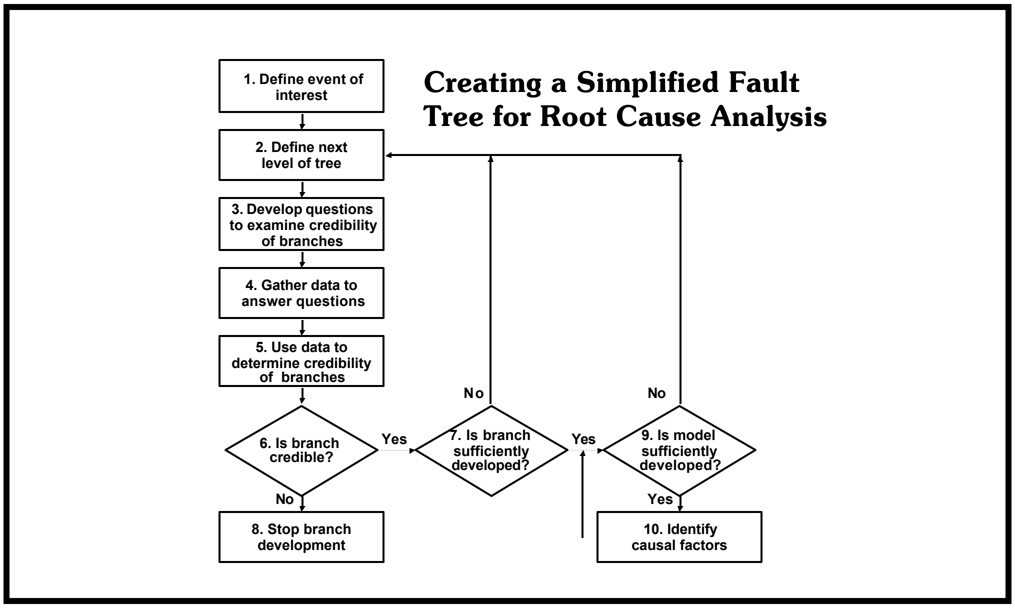
Limitations of the 5 Whys technique

The 5 Whys technique is an effective tool for determining causal factors and identifying root causes. However, it does have three primary limitations:

Brainstorming is time consuming. Compared to other techniques, the 5 Whys technique can be time consuming. The brainstorming process can be tedious for team members trying to reach consensus. This is especially true for large teams.

Results are not reproducible or consistent. Another team analyzing the same issue may reach a different solution. The brainstorming process is very difficult, if not impossible, to duplicate.

Root causes may not be identified. Like event and causal factor charting, the 5 Whys technique does not provide a means to ensure that root causes have been identified.



Creating a Simplified Fault Tree for Root Cause Analysis

1. Define event of interest
2. Define next level of tree
3. Develop questions to examine credibility of branches
4. Gather data to answer questions
5. Use data to determine credibility of branches
6. Is branch credible?
Yes
No
7. Is branch sufficiently developed?
No
Yes
8. Stop branch development
9. Is model sufficiently developed?
No
Yes
10. Identify causal factors

Creating a Simplified Fault Tree for Root Cause Analysis

The rest of this section focuses on using simple fault trees and the closely related 5 Whys analysis to conduct investigations of accidents and other undesirable events.

Step 1. Define an event of interest as the TOP event of the fault tree

Clearly describe a specific, known event of interest for which you will explore the potential underlying causes. Events such as the primary events and conditions and the secondary events and conditions can be the events of interest. Examples might be, “Flow control valve FCV-1 opened prematurely” or “The room temperature was greater than 80 °F.” Typically, the event of interest for a fault tree is an equipment or system failure or a human error.

When using a fault tree as the primary analysis tool, the accident is the TOP event.

Step 2. Define the next level of the tree

Determine the combinations of events and conditions that can cause the event to occur. If two or more events must occur to cause the event, use an AND gate and draw the events under the AND gate. For example, for a fire to exist, fuel, an oxygen source, ***and*** an ignition source must all occur simultaneously. If there are multiple ways for an event to occur, use an OR gate. For example, the fuel for a fire can be paper ***or*** gasoline.

Regardless of whether an AND gate or an OR gate is selected, this level of development is a “baby step.” It should be the smallest logical step, within reason, toward the underlying potential causes of the event above it. Taking too large a step can cause you to overlook important possibilities. Remember to include equipment failures, human errors, and external events as appropriate.

After the tree level is developed, test the tree for logic. Start with each event at the bottom of the tree. Does the logic of the tree reflect your understanding of the event or system? If an event is connected to an OR gate above, then it must be enough to cause the event above. If an event is connected to an AND gate above, is it required to cause the event above? Must ALL of the other events connected to the AND gate also occur for the event above to occur?

Step 3. Develop questions to examine the credibility of branches

Develop questions to test the credibility of each branch. What evidence would be present if this branch were true?

Step 4. Gather data to answer questions

Gather data to answer the questions that were generated in the previous step.

Step 5. Use data to determine the credibility of branches

Use the data gathered in the previous step to evaluate which branches of the tree do or do not contribute to the event of interest. Do the data support or refute the presence of this branch? Do you have sufficient information to determine the credibility of the branch? If not, you need to gather more data or continue on to the next level of the tree. Cross out any branches that you can dismiss with high confidence, and list the specific data used to make this determination beneath the crossed-out branch.

For chronic problems, assigning probabilities (i.e., percentages) to the various events will help characterize the types of events that occur most often. For chronic events, you may not be able to address every type of event that occurs, so you need to focus on those that occur most frequently. These percentages will be used in Step 6 to determine if we need to develop the event further.

If all branches leading to the event of interest through an OR gate or one or more branches leading to the event of interest through an AND gate are eliminated, either (1) the event of interest did not occur, (2) some of the data are inaccurate or were misapplied, or (3) other ways exist for the event of interest to occur.

Step 6. Is the branch credible?

Determine if the branch is credible. For acute problems, if the branch is credible, continue on to Step 7. If the branch is not credible, proceed to Step 8. For chronic problems, if the percentage of events for this branch is high, continue on to Step 7. If the percentage of events for this branch is low, proceed to Step 8.

Step 7. Is the branch sufficiently developed?

Determine if the branch is sufficiently developed. The branch is complete when it is detailed enough to allow an understanding of how the top event occurs. If the branch is not complete, return to Step 2. If the branch is complete, move on to Step 9.

Step 8. Stop branch development

There is no reason to develop the branch further if you have determined it is not credible. Stop development of this branch and move on to Step 9.

Step 9. Stop when the scenario model is "complete"

The model is complete when you have a clear understanding of how the accident occurred. Keep your model "barely adequate" for identifying the issues of concern for your analysis; avoid unnecessary detail or resolution that will not influence your results. For acute problems, if you have more than one possible way for the event of interest to have occurred and cannot gather data to dismiss any of the remaining possibilities, you should consider each as a potential causal factor and make recommendations to prevent each. For chronic problems, you will typically need to address a number of primary contributors to the event of interest.

Step 10. Identify causal factors (optional)

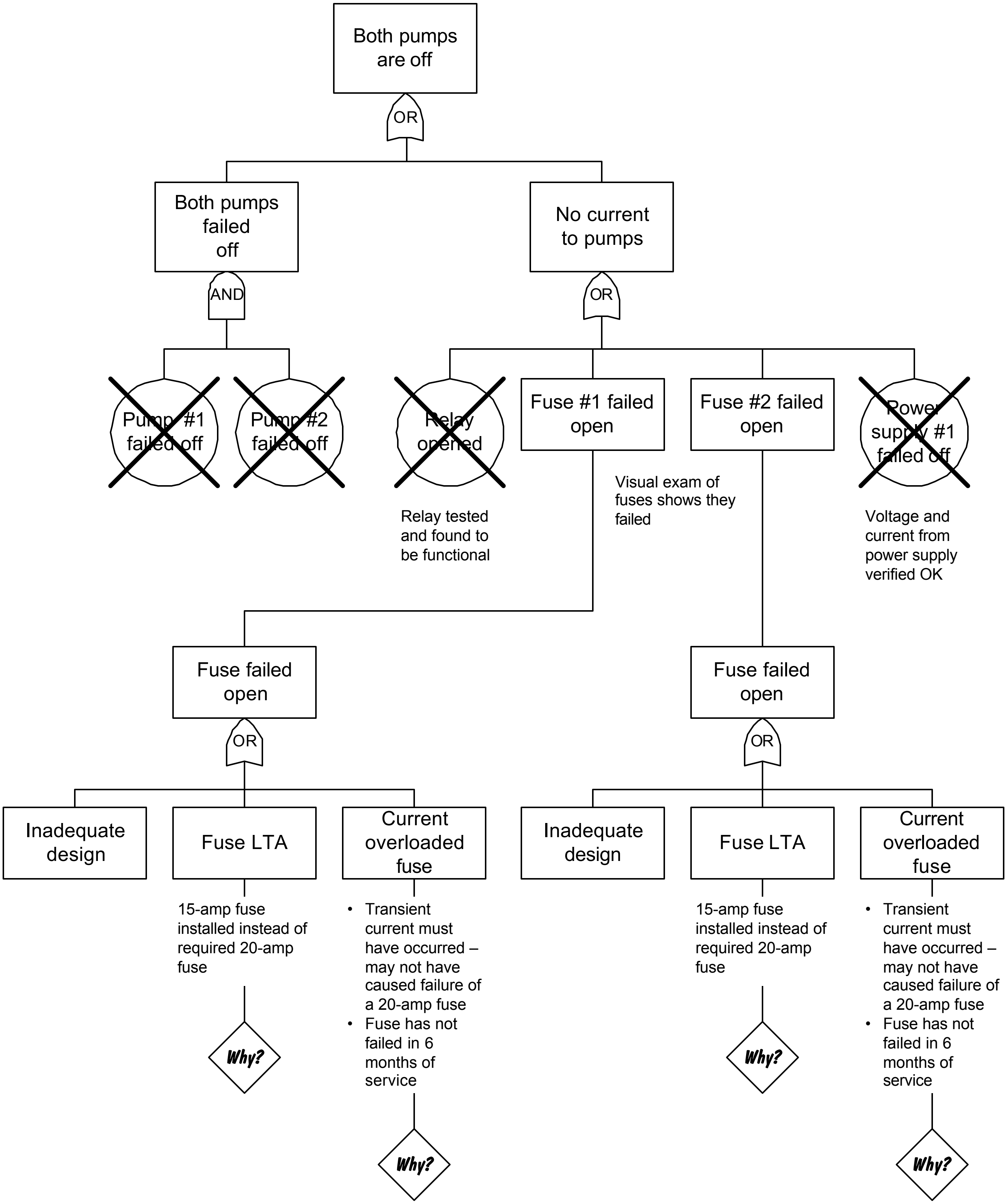
If the fault tree method is being used as the primary analysis tool, causal factors should be identified.

Remember, you need not be, and probably will not be, the subject matter expert for the analysis. Use the expertise of others to help you develop the fault tree structure and apply the known data to dismiss branches appropriately.

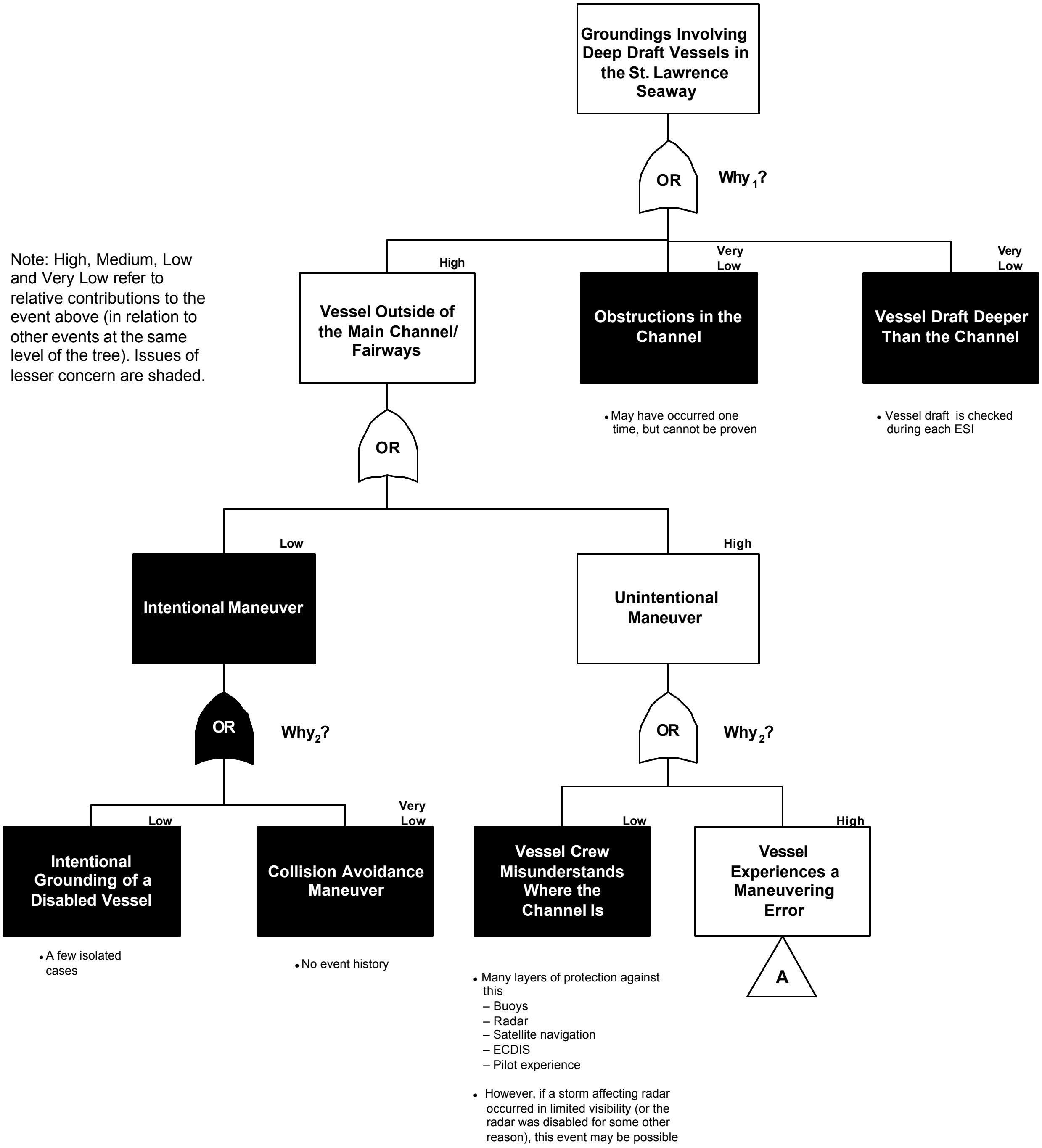
Use Post-it® Notes to "draw" the tree

- Allows for rapid revision of the tree
- Use different colors for different items
  - green (events)
  - yellow (OR gates)
  - pink (AND gates)

Example of fault tree analysis in an investigation of one specific event


Both pumps are off
OR
Both pumps failed off
No current to pumps
AND
OR
Pump #1 failed off
Pump #2 failed off
Relay opened
Fuse #1 failed open
Fuse #2 failed open
Power supply #1 failed off
Relay tested and found to be functional
Visual exam of fuses shows they failed
Voltage and current from power supply verified OK
Fuse failed open
Fuse failed open
OR
OR
Inadequate design
Fuse LTA
Current overloaded fuse
Inadequate design
Fuse LTA
Current overloaded fuse
15-amp fuse installed instead of required 20-amp fuse
• Transient current must have occurred – may not have caused failure of a 20-amp fuse
• Fuse has not failed in 6 months of service
15-amp fuse installed instead of required 20-amp fuse
• Transient current must have occurred – may not have caused failure of a 20-amp fuse
• Fuse has not failed in 6 months of service
Why?
Why?
Why?
Why?

Example of fault tree analysis in an investigation of a chronic problem


Groundings Involving Deep Draft Vessels in the St. Lawrence Seaway
OR
Why $_1$?
High
Vessel Outside of the Main Channel/ Fairways
Very Low
Obstructions in the Channel
Very Low
Vessel Draft Deeper Than the Channel
OR
Low
Intentional Maneuver
High
Unintentional Maneuver
OR
Why$_2$?
OR
Why$_2$?
Low
Intentional Grounding of a Disabled Vessel
Very Low
Collision Avoidance Maneuver
Low
Vessel Crew Misunderstands Where the Channel Is
High
Vessel Experiences a Maneuvering Error
A

Note: High, Medium, Low and Very Low refer to relative contributions to the event above (in relation to other events at the same level of the tree). Issues of lesser concern are shaded.

- May have occurred one time, but cannot be proven

- Vessel draft is checked during each ESI

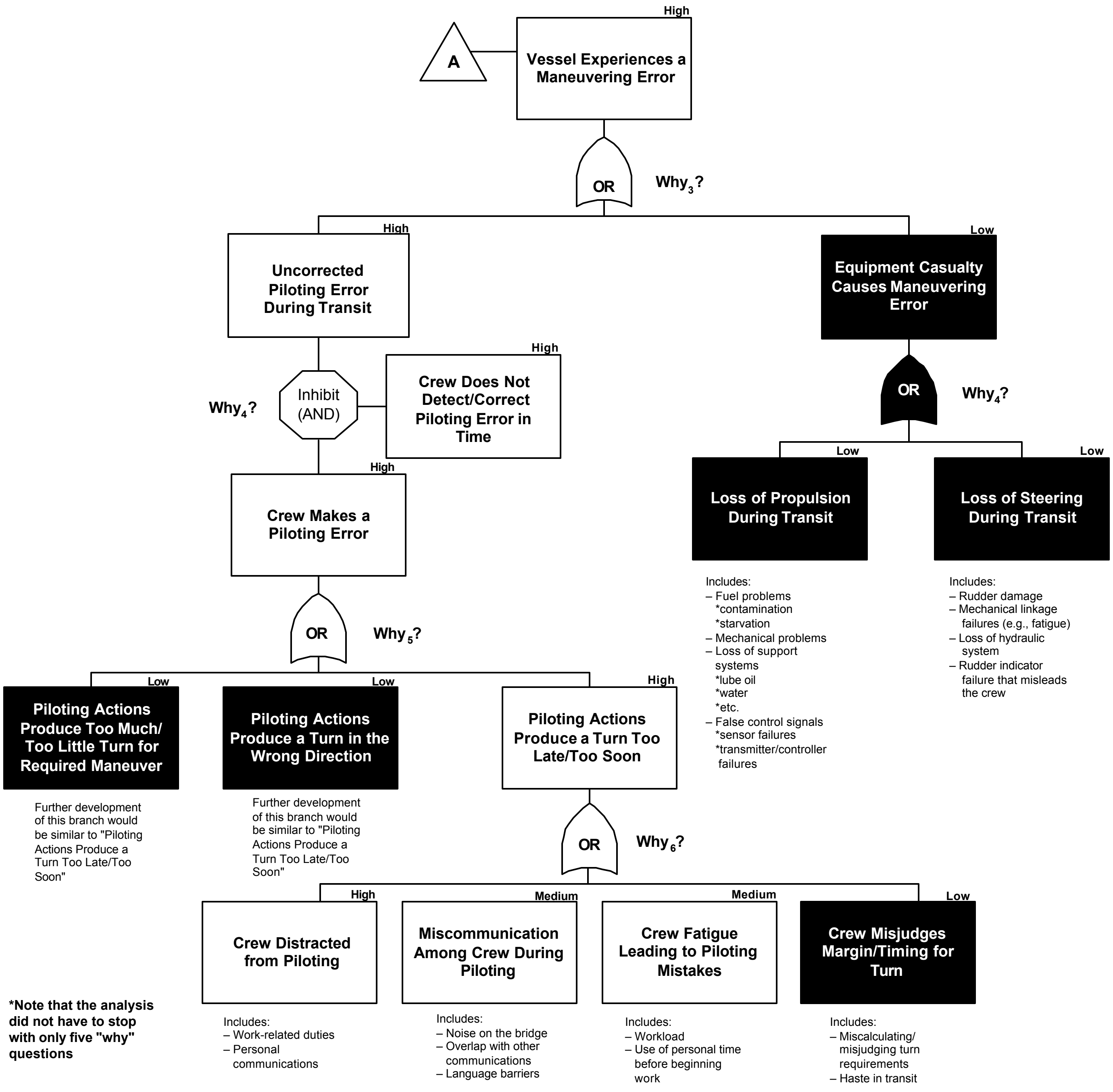
- A few isolated cases

- No event history

- Many layers of protection against this
  - Buoys
  - Radar
  - Satellite navigation
  - ECDIS
  - Pilot experience

- However, if a storm affecting radar occurred in limited visibility (or the radar was disabled for some other reason), this event may be possible

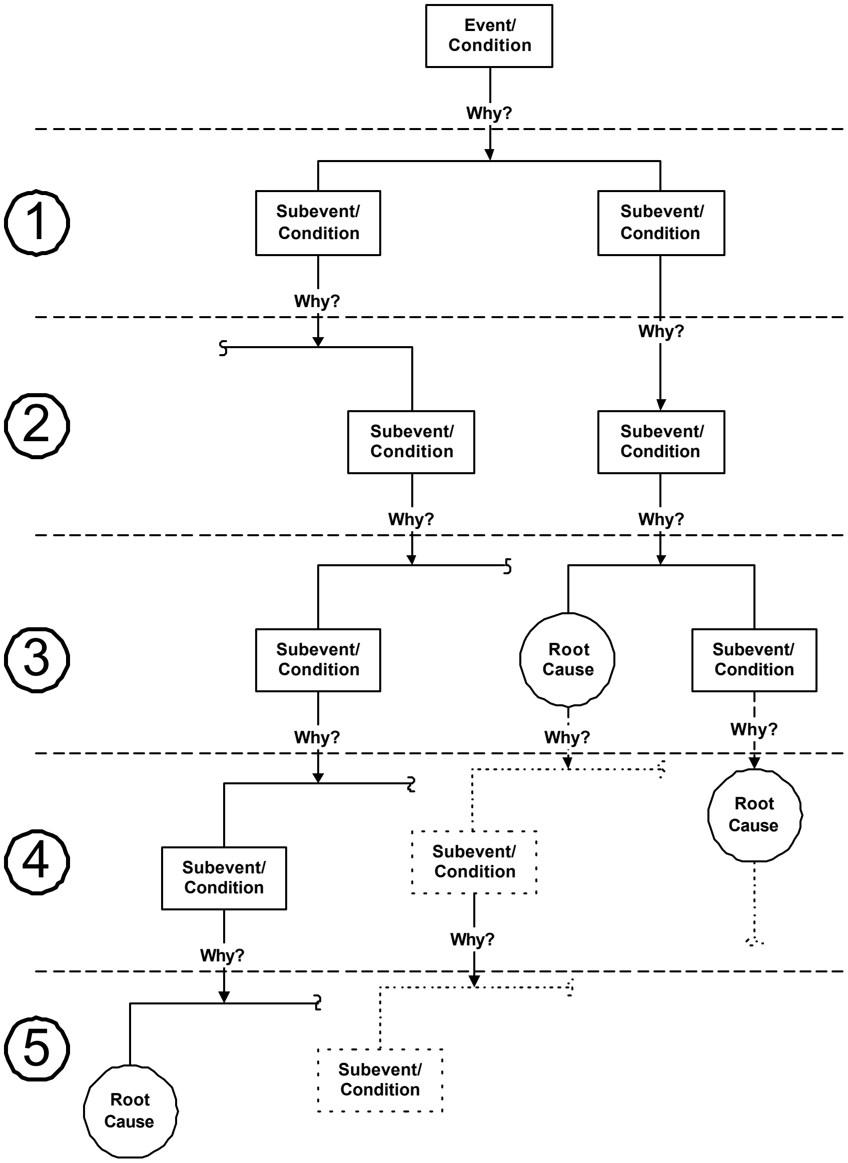
Example of fault tree analysis in an investigation of a chronic problem (cont.)


A
High
Vessel Experiences a Maneuvering Error
OR
Why$_3$?
High
Uncorrected Piloting Error During Transit
Low
Equipment Casualty Causes Maneuvering Error
High
Crew Does Not Detect/Correct Piloting Error in Time
Why$_4$?
Inhibit (AND)
OR
Why$_4$?
High
Crew Makes a Piloting Error
Low
Loss of Propulsion During Transit
Low
Loss of Steering During Transit
Includes:
– Fuel problems
*contamination
*starvation
– Mechanical problems
– Loss of support systems
*lube oil
*water
*etc.
– False control signals
*sensor failures
*transmitter/controller failures
Includes:
– Rudder damage
– Mechanical linkage failures (e.g., fatigue)
– Loss of hydraulic system
– Rudder indicator failure that misleads the crew
OR
Why$_5$?
Low
Piloting Actions Produce Too Much/ Too Little Turn for Required Maneuver
Low
Piloting Actions Produce a Turn in the Wrong Direction
High
Piloting Actions Produce a Turn Too Late/Too Soon
Further development of this branch would be similar to "Piloting Actions Produce a Turn Too Late/Too Soon"
Further development of this branch would be similar to "Piloting Actions Produce a Turn Too Late/Too Soon"
OR
Why$_6$?
High
Crew Distracted from Piloting
Medium
Miscommunication Among Crew During Piloting
Medium
Crew Fatigue Leading to Piloting Mistakes
Low
Crew Misjudges Margin/Timing for Turn
Includes:
– Work-related duties
– Personal communications
Includes:
– Noise on the bridge
– Overlap with other communications
– Language barriers
Includes:
– Workload
– Use of personal time before beginning work
Includes:
– Miscalculating/ misjudging turn requirements
– Haste in transit

***Note that the analysis did not have to stop with only five "why" questions**

Conclusions about 5 Whys

- Resulting subevents and conditions should be at or near the root causes of the event
- More or less detailed evaluation may be necessary for some cases to reach management system root causes
- Judgment and experience are key factors in selecting the right level of evaluation and the completeness of results
- This technique can be time consuming compared to techniques that do not require brainstorming
- This technique works, even when the management systems are ill defined
- The results are not reproducible or consistent, but the application is auditable


Event/ Condition
Why?
1
Subevent/ Condition
Subevent/ Condition
Why?
Why?
2
Subevent/ Condition
Subevent/ Condition
Why?
Why?
3
Subevent/ Condition
Root Cause
Subevent/ Condition
Why?
Why?
Why?
4
Subevent/ Condition
Subevent/ Condition
Root Cause
Why?
Why?
5
Root Cause
Subevent/ Condition