Fault Tree Analysis

What is it?

Fault Tree Analysis (definition)

A technique by which conditions and factors that can contribute to a specified undesired event are identified and organized in a logical manner and represented pictorially.

Fault Tree Analysis - technique

Starting with the undesired (top) event the possible causes of that event are identified at the next lower level. If each of those contributors could produce the top event alone an OR gate is used; if all the contributors must act to result in the top event an AND gate is used. Then continue to the next level.

Fault Tree Analysis

A tool to investigate a problem

Where you keep asking the question :

What could cause that??

Event Tree Analysis

A tool to investigate a problem starting with a condition or event

Where you keep asking the question :

What could this cause? or

What could result?

Event Tree Analysis (definition)

A technique that is used to identify the possible outcomes given the occurrence of an initiating event (or given event).

Event Tree Analysis

PFMA - uses this approach in looking for and identifying potential failure modes.

Fault Tree Analysis

What does it provide ?

A Fault Tree Analysis - Like an Event Tree Analysis - Provides

- A tool to help analyze a problem
- A means to identify the components of a problem
- A tool to stimulate thinking
- Increased Understanding of the potential problem

Fault Tree Analysis

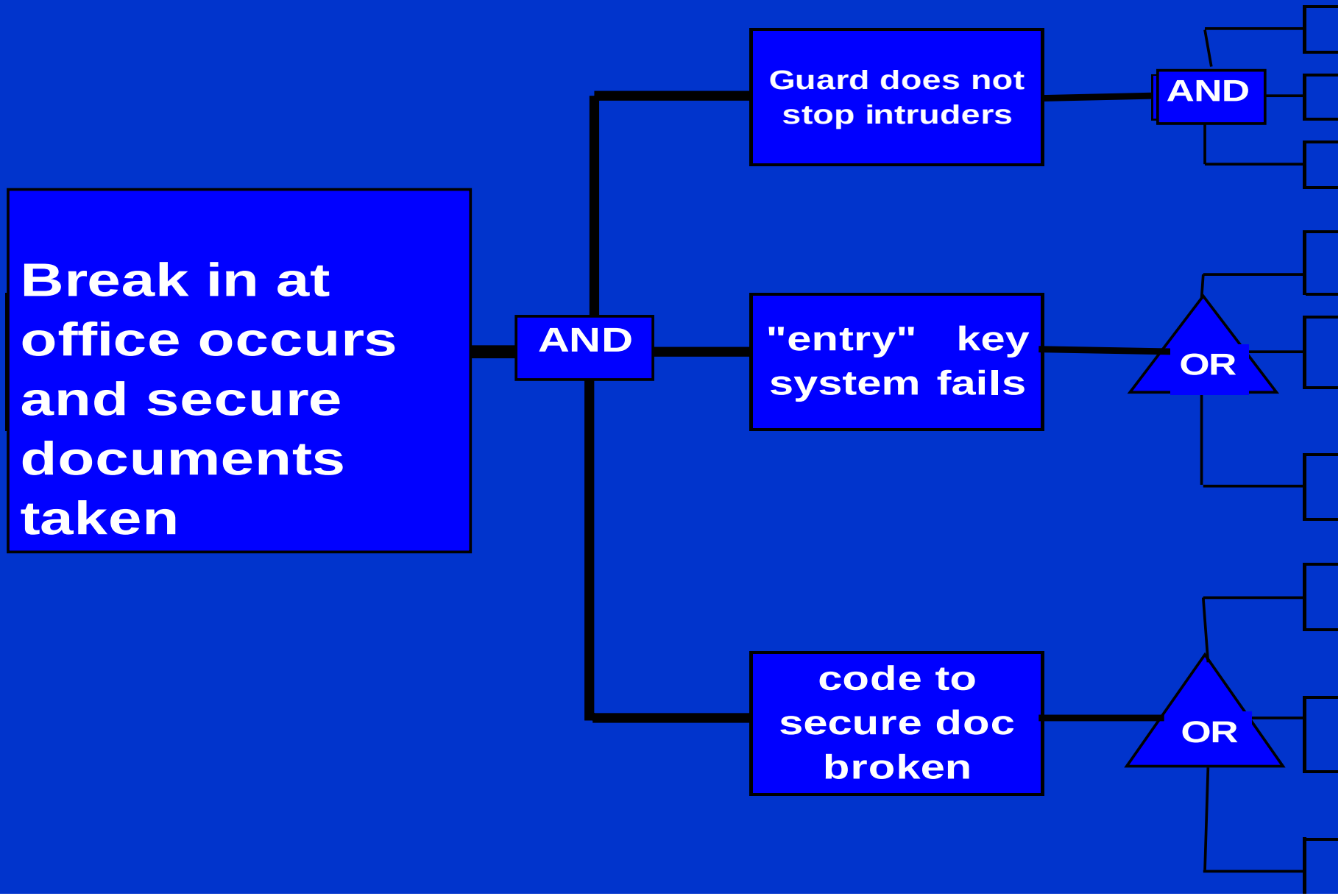
Why use it for Pumped Storage Projects?

Performing a Fault Tree Analysis

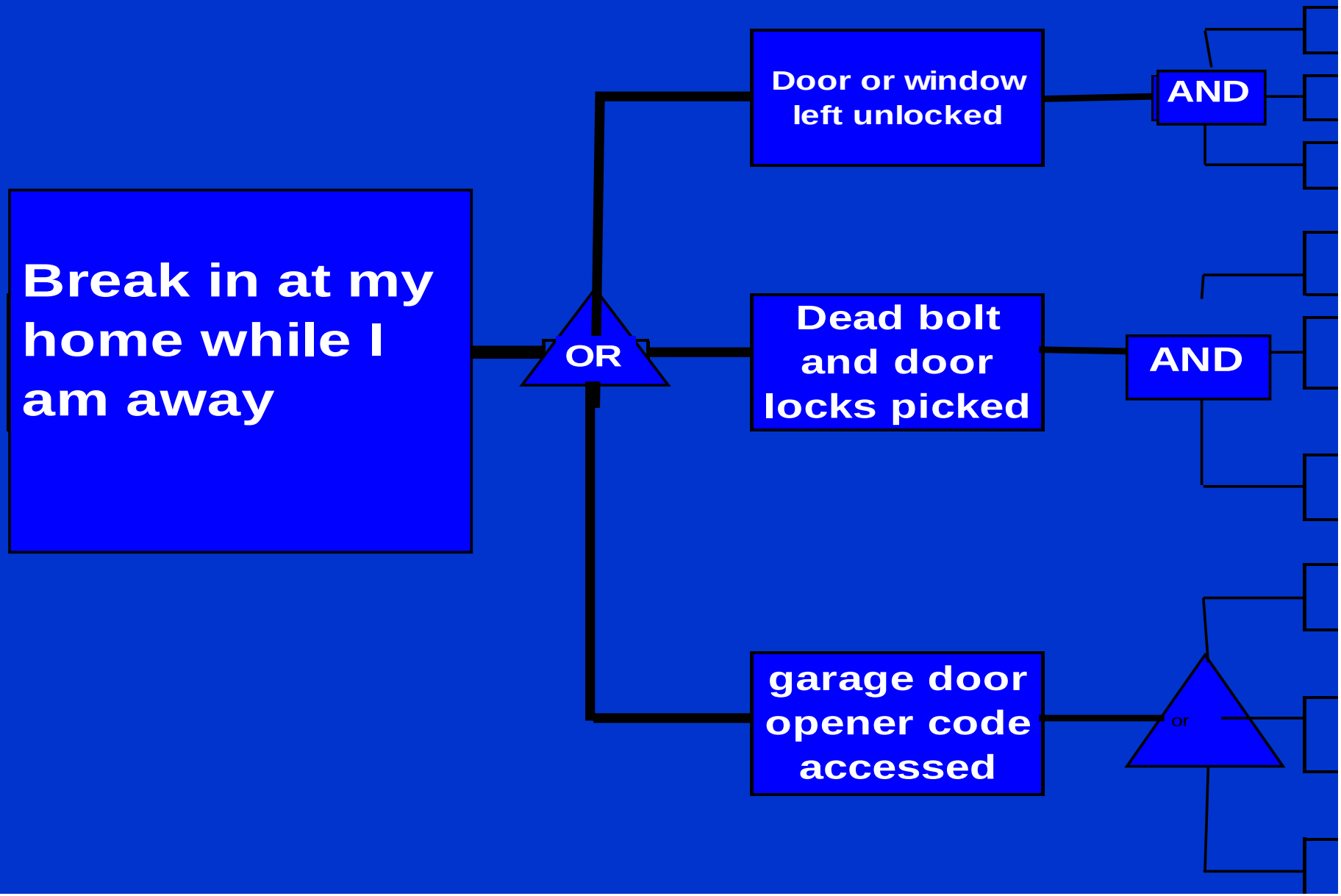
Fault Tree Analysis - technique

Starting with the undesired (top) event the possible causes of that event are identified at the next lower level. If each of those contributors could produce the top event alone an OR gate is used; if all the contributors must act to result in the top event an AND gate is used. Then continue to the next level.

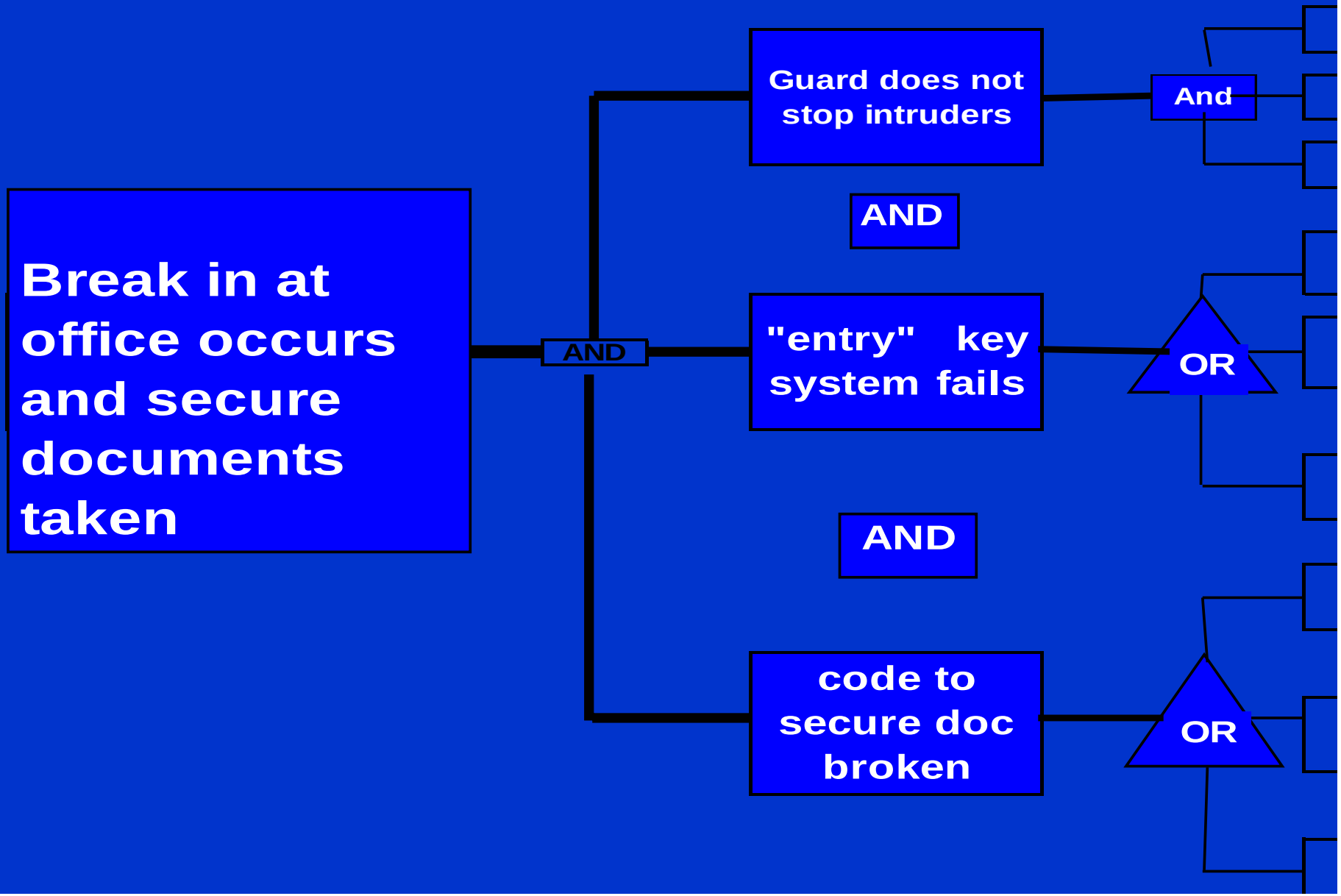
Example “AND” Gate



Example “OR” Gate



Example “And” Gate Scenario



Fault Tree Analysis for Over-pumping at Pump Storage Project

Top Event

Statement of the Failure or Problem

being investigated

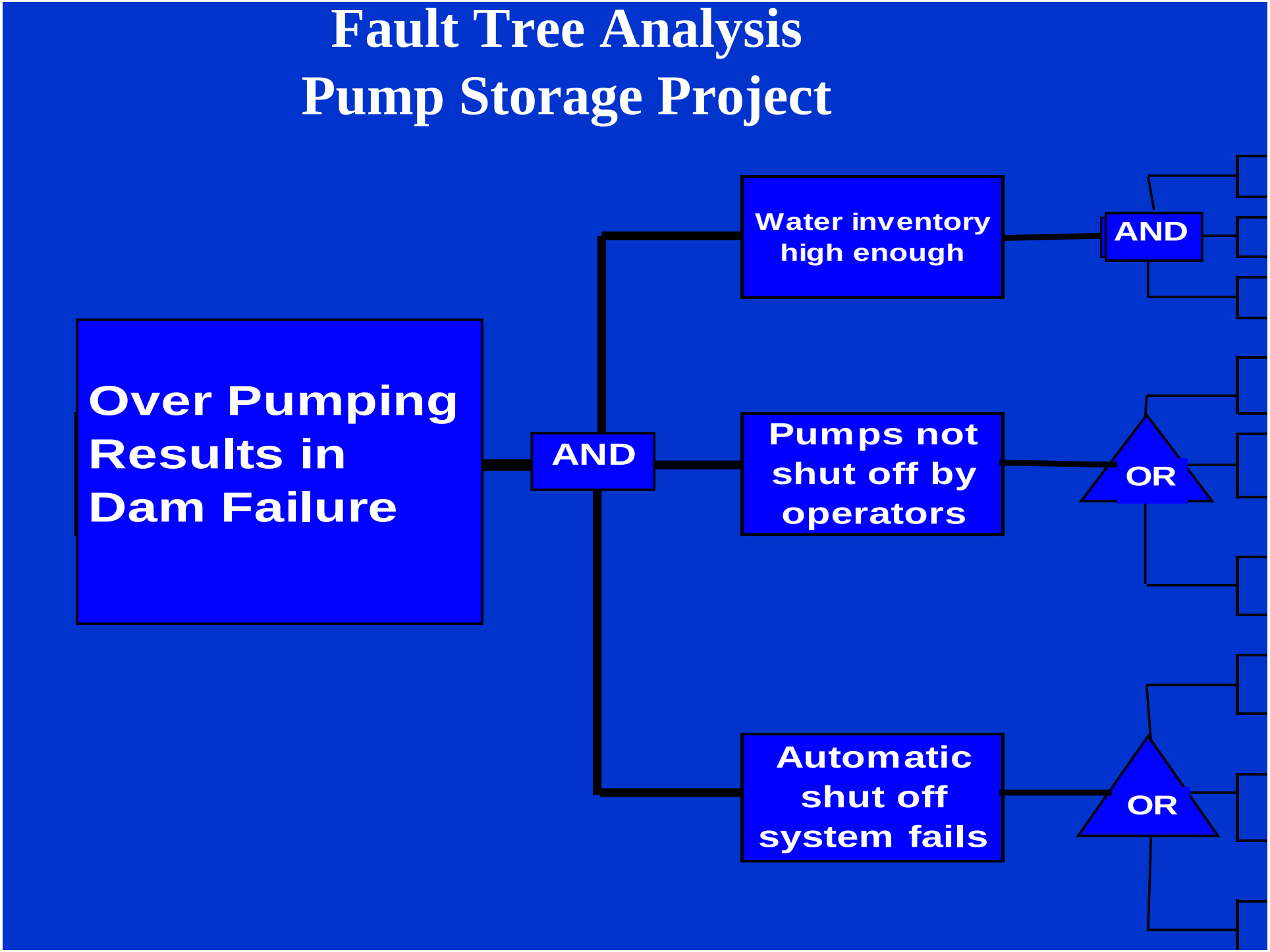
Water is pumped from the Lower Reservoir to the Upper Reservoir until the Upper Reservoir dam overtops and the Dam is breached.

Next - Ask:
What has to happen for that adverse event to occur?

Answer ---

- There has to be enough water in system to overfill, and
- The Operators have to fail to shut off the pumps, and
- The automatic shut off system has to fail to work

Fault Tree Analysis
Pump Storage Project



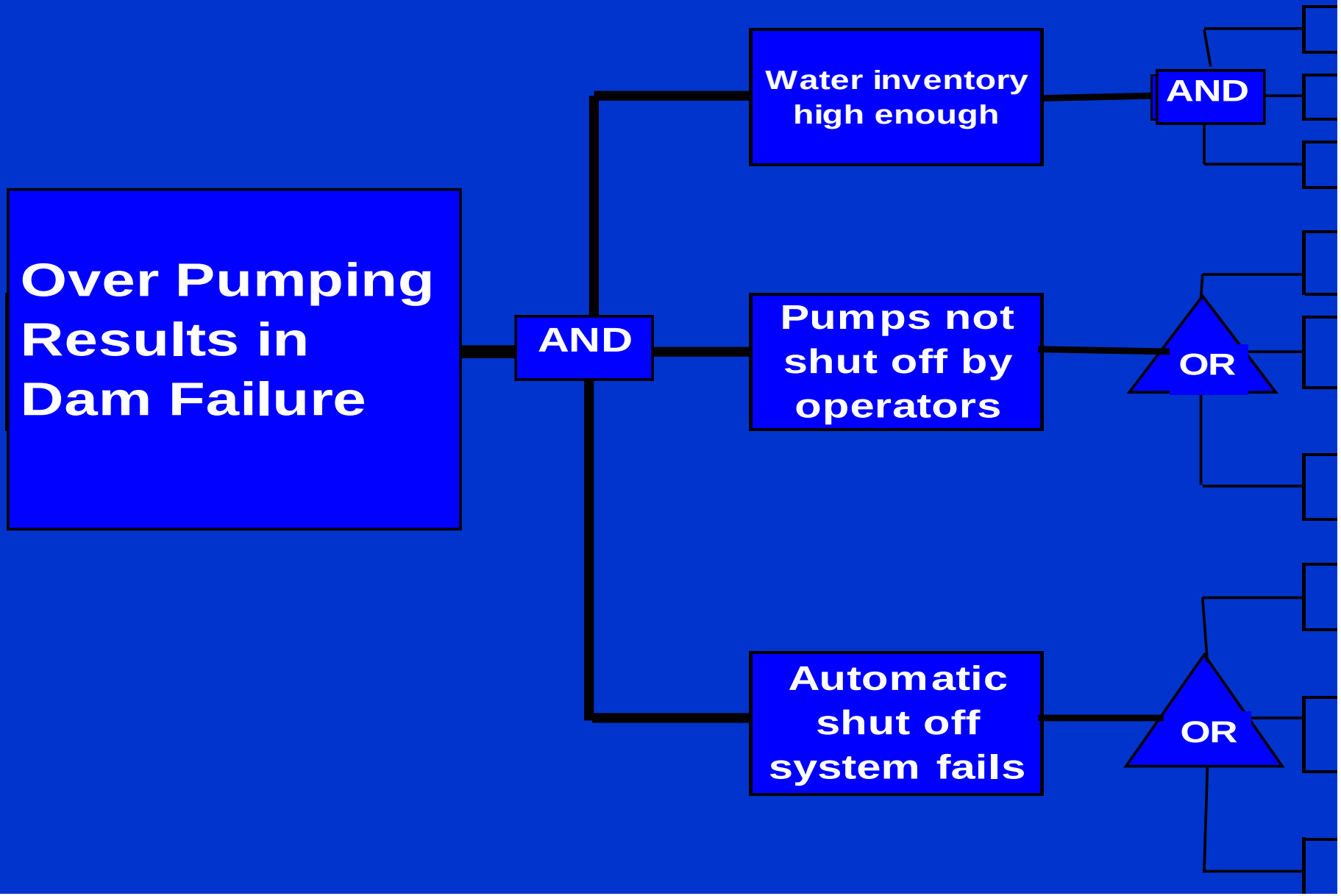
Then Ask - What has to happen for each of those conditions to occur?

Actually the analysis of the potential for Over-pumping started with a list of questions / issues for the operators to get answers for / discuss / consider prior to the Fault Tree Analysis :

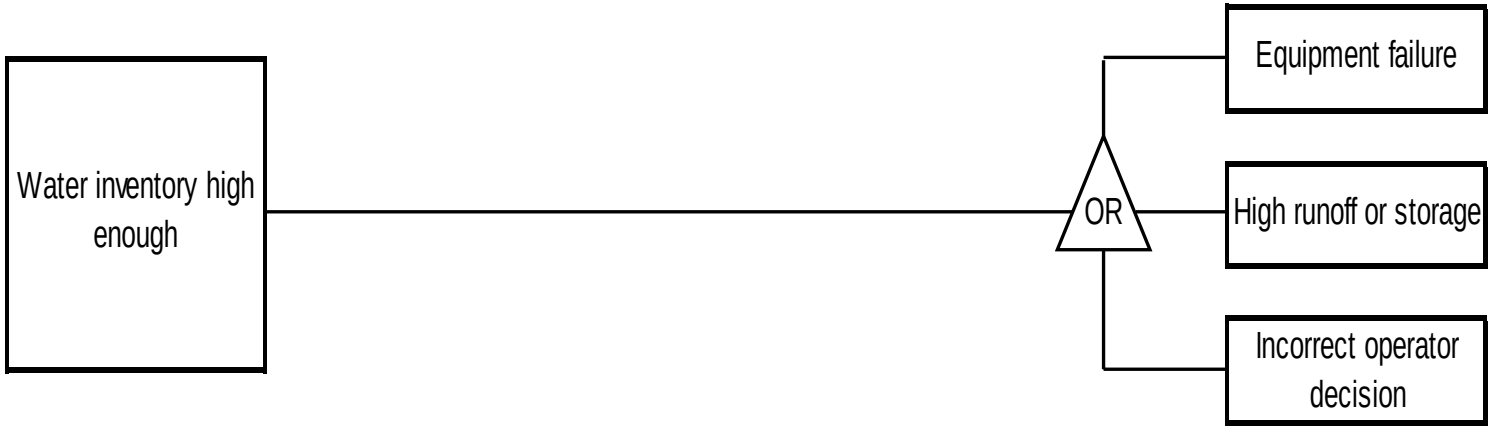
The Fault Tree Analysis of the potential for Over-pumping started with discussion of:

1. **Water inventory**
2. **Typical operation and procedures**
3. **Alarms and auto shut off system**

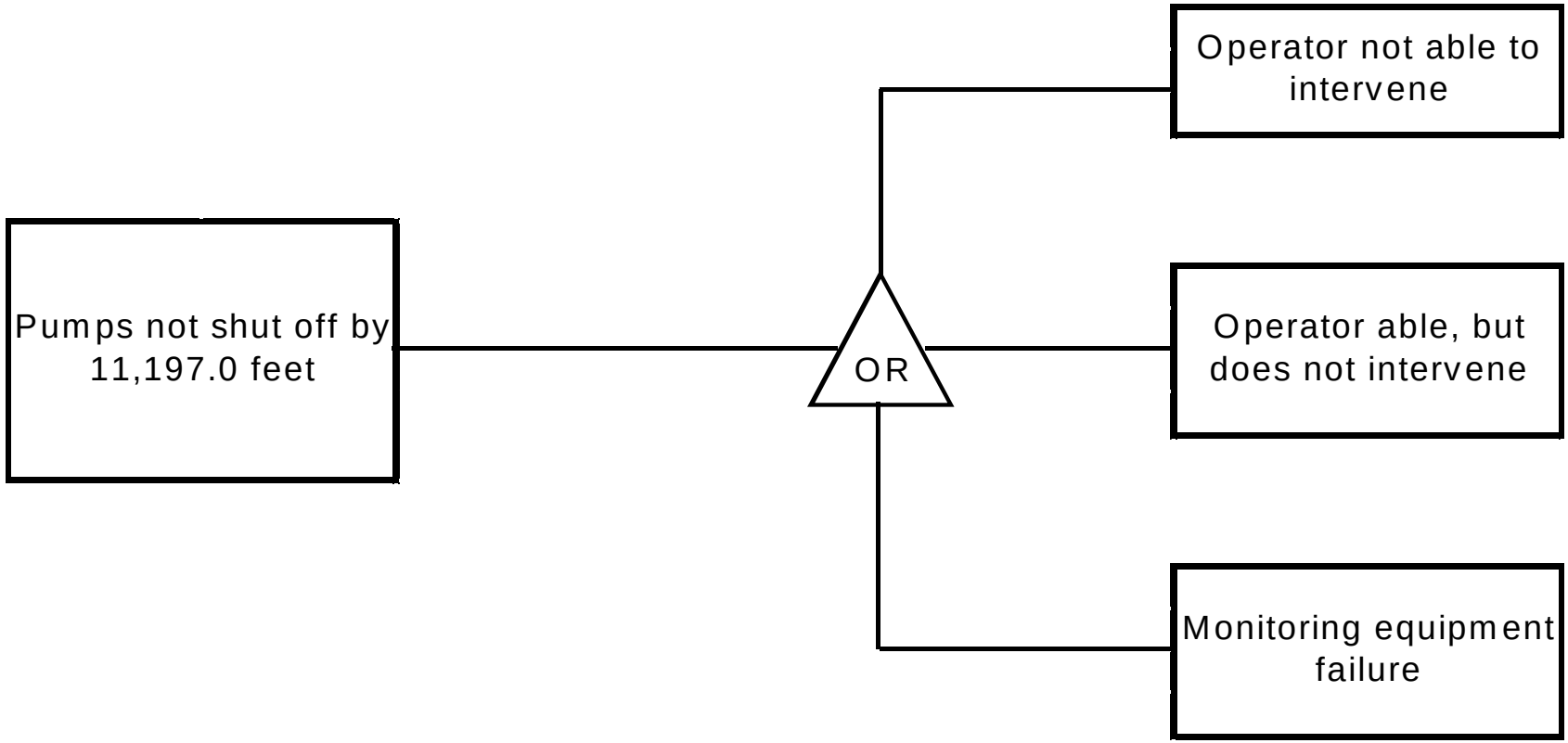
Fault Tree Analysis
Pump Storage Project



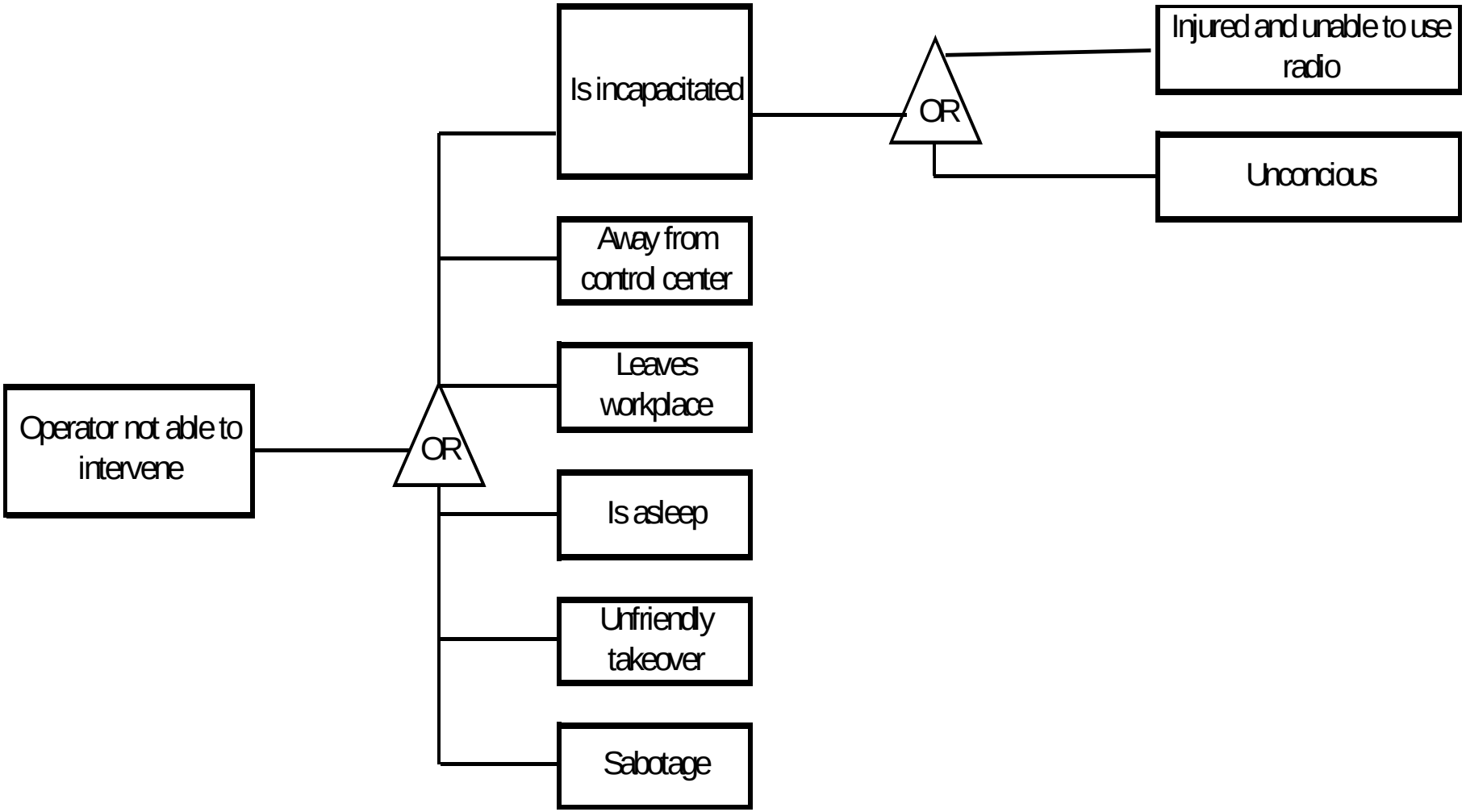
List of Potential Enhancements / Action Items is Maintained during Discussions


Water inventory high enough
OR
Equipment failure
High runoff or storage
Incorrect operator decision

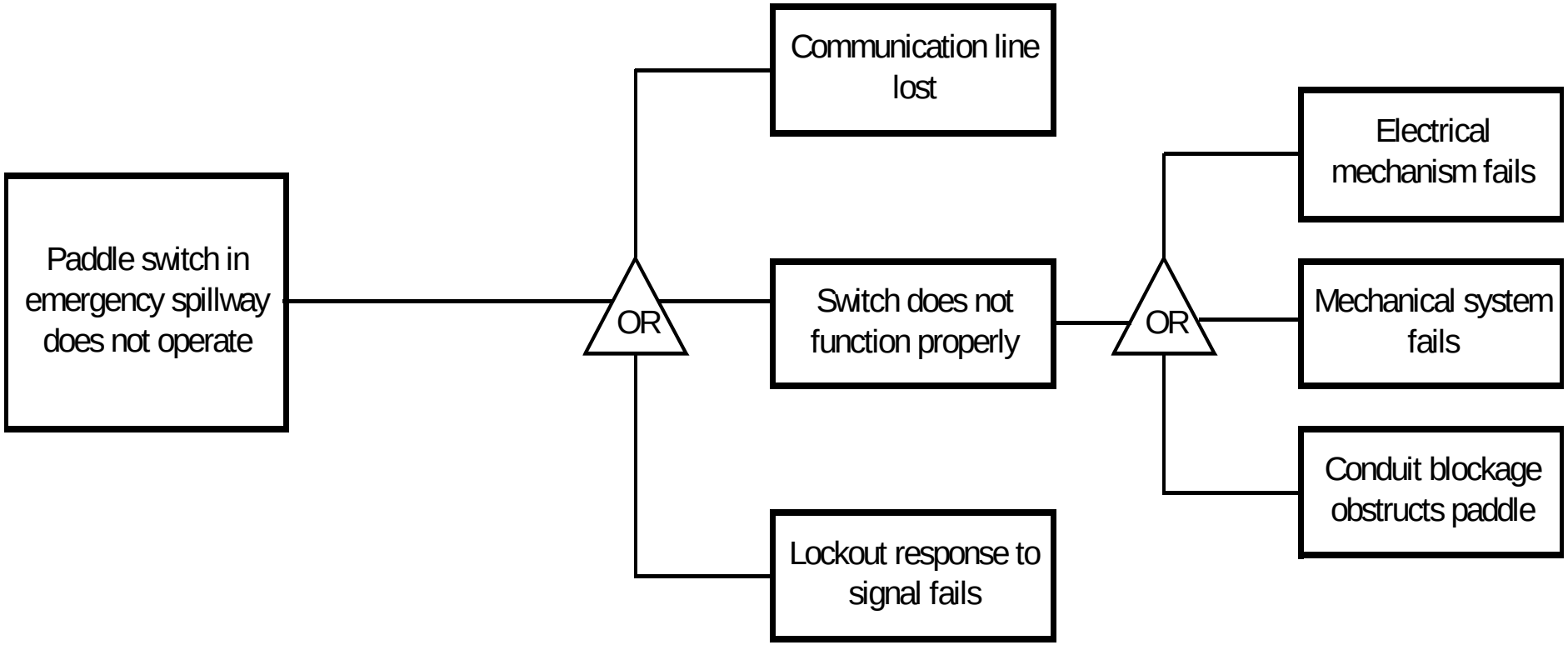
Pumps Are Not Shut Off



Operator Not Able To Intervene



Automatic Shutoff Fails



Major Findings From Discussions

- Only under uncommon water / operating conditions is there enough water to allow overtopping
- Operators work out allowable pumping time
- Two other entities monitor conditions at site
- Power to alarms / controls are vulnerable

Evaluation of Credible Scenarios

After all the discussions were complete, the team assessed what scenario(s) among all the possibilities discussed were really credible

Credible Scenario 1

- *The first credible scenario would be for an operator to become incapacitated or to deliberately walk off the job without informing anyone else. This event, however, would not result in over-pumping unless (1) water inventory was high, (2)the paddle switch failed and (3)there was no intervention from others*

Credible Scenario 2

- *The second credible scenario is that the communication line from the upper reservoir is down. This eliminates the alarms and paddle switch shut off. The water level would have to be high and the operator would have to not be available or not fulfilling function for this to lead to failure.*

Credible Scenario 3

The third credible scenario is that the primary power to the upper reservoir fails since it is an overhead power line and has failed in the past. However, with DC power being provided for several of the instruments, it would require a combination of both communication and power supply losses to become a problem for monitoring the upper reservoir instrumentation.

FTA: OVER PUMPING
MAJOR FINDINGS & UNDERSTANDING

- Designed for remote operations
- Redundant Monitoring Instrumentation
- Control center reservoir alarms visual and audible—checked each shift
- Current water level operated 6 feet below top of dam
- Duration & quantity of overtopping water for rock fill dam important
- Low probability of high water levels in both reservoirs simultaneously
- No history of over pumping except initial start-up
- Telemetry cables to upper reservoir vulnerable
- Tailwater monitoring only visually via camera
- Emergency spillway overflow paddle switch tested annually
- Power supply backup needs to be reevaluated
- Powerhouse control center, AGC & Marketing staffed 24/7
- Communication with AGC & Marketing—every 2 hours minimum
- Pump/Generation cycles manually checked by operator
- Operator record computed pump back time on white board in control center
- Pump/Generation cycles monitored also monitored by AGC & Marketing
- Human factor---weak link

Conclusion

As with the PFMA the Fault Tree Analysis provides a good vehicle for :

- **improving project understanding**
- **identifying potential problem areas and potential actions to reduce risk**

Fault Tree Analysis Exercise

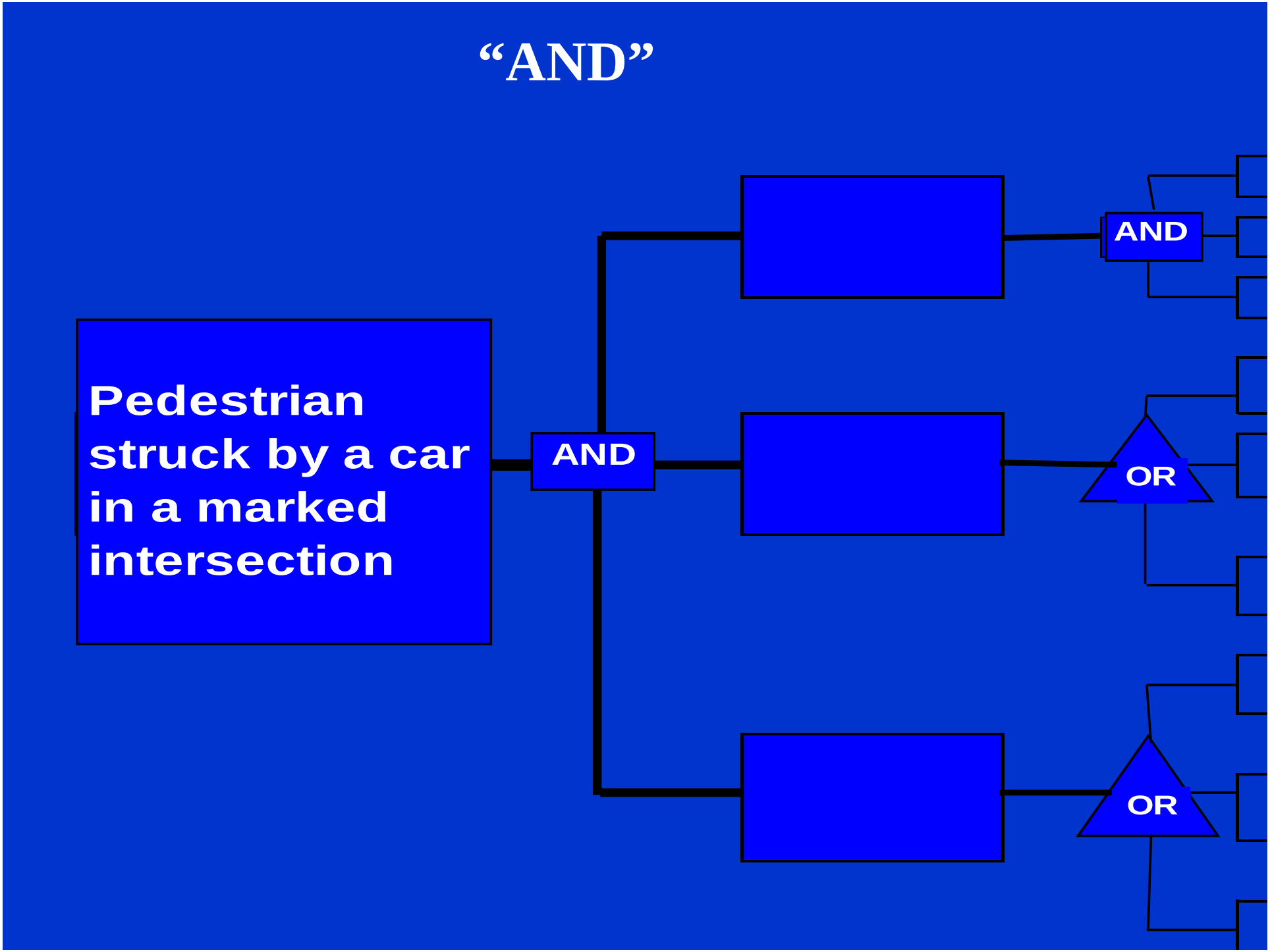
Adverse Event

- Pedestrian is struck by a car in an intersection which has a marked cross walk

Assignment - fill in the first level of causes

use AND factors or OR factors as you decide

“AND”


Pedestrian struck by a car in a marked intersection
AND
AND
OR
OR

“OR” Gate Choice