Fault Tree Analysis

P.L. Clemens

February 2002

4th Edition

Topics Covered

- Fault Tree Definition
- Developing the Fault Tree
- Structural Significance of the Analysis
- Quantitative Significance of the Analysis
- Diagnostic Aids and Shortcuts
- Finding and Interpreting Cut Sets and Path Sets
- Success-Domain Counterpart Analysis
- Assembling the Fault Tree Analysis Report
- Fault Tree Analysis vs. Alternatives
- Fault Tree Shortcoming/Pitfalls/Abuses

All fault trees appearing in this training module have been drawn, analyzed, and printed using FaultrEase^{TM}, a computer application available from: Arthur D. Little, Inc./Acorn Park/ Cambridge, MA., 02140-2390 – Phone (617) 864-5770.

First – A Bit of Background

- Origins of the technique
- Fault Tree Analysis defined
- Where best to apply the technique
- What the analysis produces
- Symbols and conventions

JACOBS SVERDRUP

Origins

- Fault tree analysis was developed in 1962 for the U.S. Air Force by Bell Telephone Laboratories for use with the Minuteman system…was later adopted and extensively applied by the Boeing Company…is one of many symbolic logic analytical techniques found in the operations research discipline.

JACOBS SVERDRUP

The Fault Tree is

- A graphic "model" of the **pathways** within a system that can lead to a **foreseeable, undesirable loss event**. The pathways interconnect contributory events and conditions, using **standard logic symbols**. Numerical probabilities of occurrence **can** be entered and propagated through the model to evaluate probability of the foreseeable, undesirable event.
- Only one of many System Safety analytical tools and techniques.

Fault Tree Analysis is Best Applied to Cases with

- Large, perceived threats of loss, i.e., high risk.
- Numerous potential contributors to a mishap.
- Complex or multi-element systems/processes.
- Already-identified undesirable events. (a must!)
- Indiscernible mishap causes (i.e., autopsies).

Caveat: Large fault trees are resource-hungry and should not be undertaken without reasonable assurance of need.

JACOBS SVERDRUP

Fault Tree Analysis Produces

- Graphic display of chains of events/conditions leading to the loss event.
- Identification of those potential contributors to failure that are “critical.”
- Improved understanding of system characteristics.
- Qualitative/quantitative insight into probability of the loss event selected for analysis.
- Identification of resources committed to preventing failure.
- Guidance for redeploying resources to optimize control of risk.
- Documentation of analytical results.

JACOBS SVERDRUP

Some Definitions

– **FAULT**
  - An abnormal undesirable state of a system or a system element* induced 1) by presence of an improper command or absence of a proper one, or 2) by a failure (see below). All failures cause faults; not all faults are caused by failures. A system which has been shut down by safety features has not faulted.

– **FAILURE**
  - Loss, by a system or system element*, of functional integrity to perform as intended, e.g., relay contacts corrode and will not pass rated current closed, or the relay coil has burned out and will not close the contacts when commanded – the relay has <u>failed</u>; a pressure vessel bursts – the vessel fails. A protective device which functions as intended has <u>not</u> failed, e.g, a blown fuse.

---

*System *element*: a subsystem, assembly, component, piece part, etc.

– **PRIMARY (OR BASIC) FAILURE**

- The failed element has seen no exposure to environmental or service stresses exceeding its ratings to perform. E.g., fatigue failure of a relay spring within its rated lifetime; leakage of a valve seal within its pressure rating.

– **SECONDARY FAILURE**

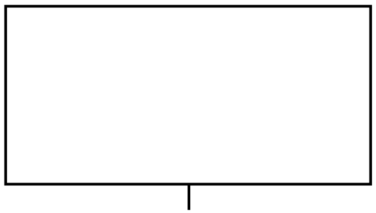
- Failure induced by exposure of the failed element to environmental and/or service stresses exceeding its intended ratings. E.g., the failed element has been improperly designed, or selected, or installed, or calibrated for the application; the failed element is overstressed/underqualified for its burden.

Assumptions and Limitations

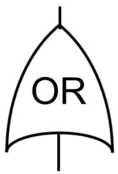
- Non-repairable system.
- No sabotage.
- Markov…
  - Fault rates are constant… λ = 1/MTBF = K
  - The future is independent of the past – i.e., future states available to the system depend only upon its present state and pathways now available to it, not upon how it got where it is.
- Bernoulli…
  - Each system element analyzed has two, mutually exclusive states.

JACOBS SVERDRUP

The Logic Symbols

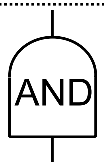


TOP Event – forseeable, undesirable event, toward which all fault tree logic paths flow,or **Intermediate event** – describing a system state produced by antecedent events.

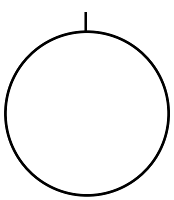


"Or" Gate – produces output if any input exists. Any input, individual, must be (1) necessary and (2) sufficient to cause the output event.

Most Fault Tree Analyses can be carried out using only these four symbols.



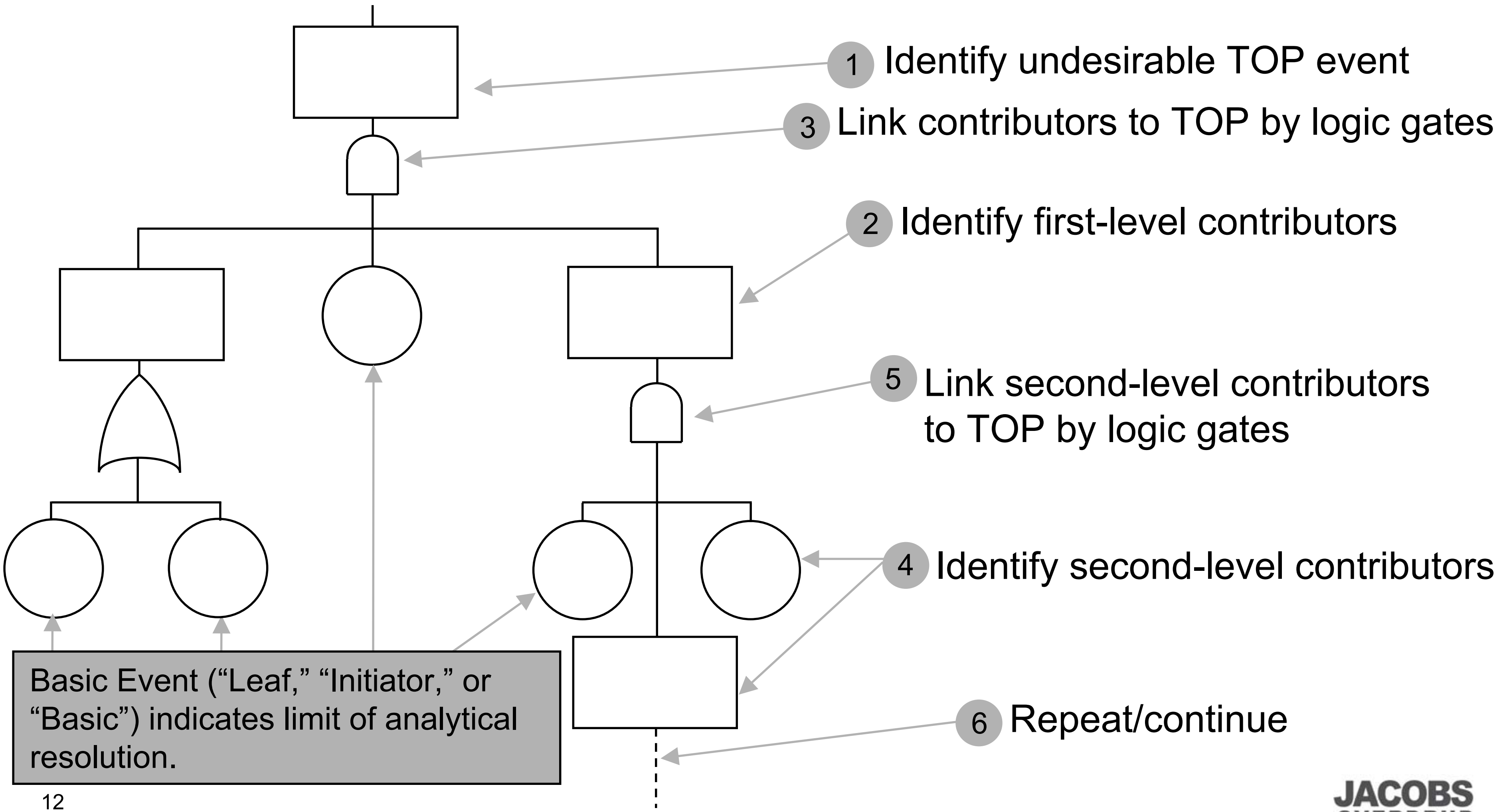
"And" Gate – produces output if all inputs co-exist. All inputs, individually must be (1) necessary and (2) sufficient to cause the output event



Basic Event – Initiating fault/failure, not developed further. (Called "Leaf," "Initiator," or "Basic.") The Basic Event marks the limit of resolution of the analysis.

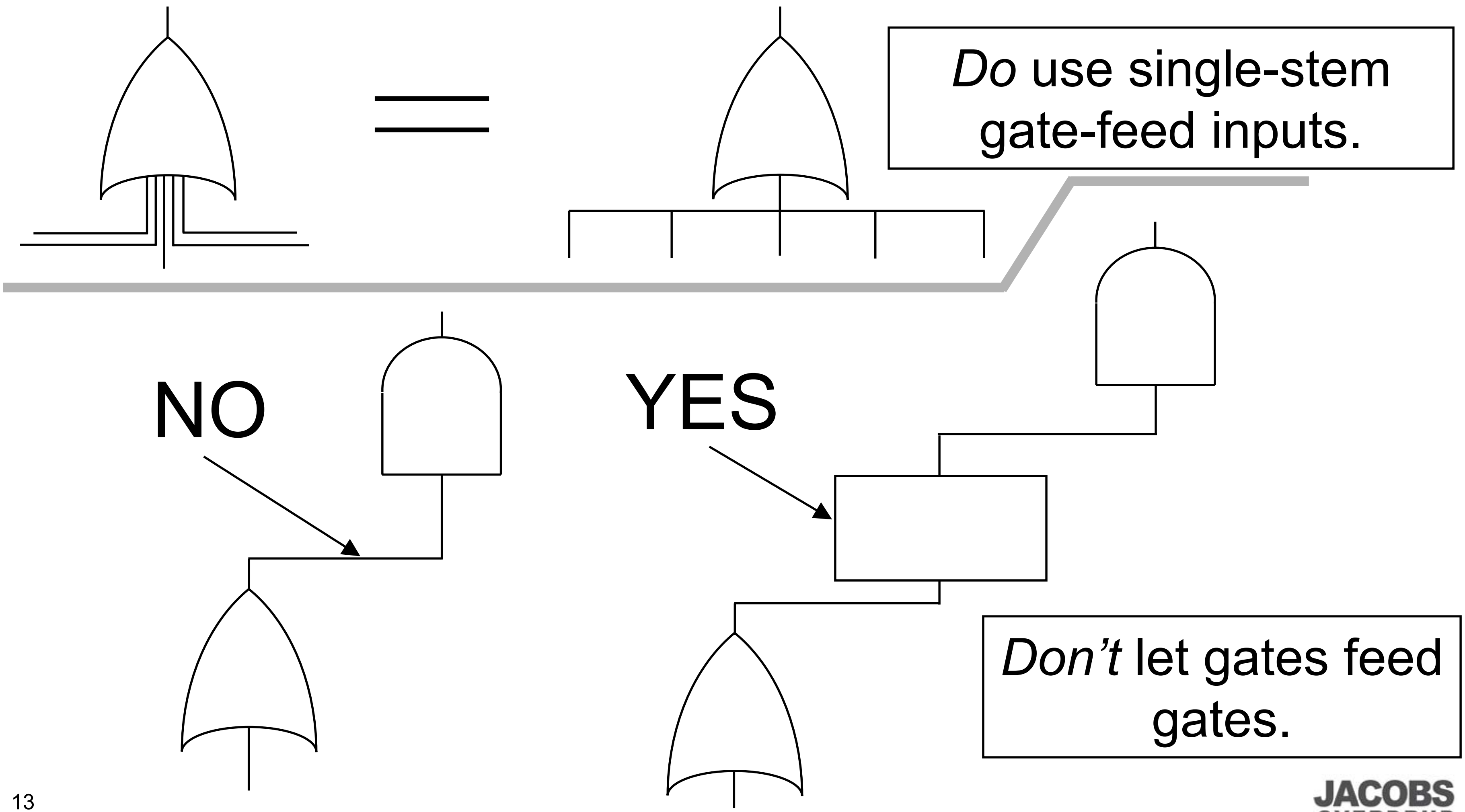
Events and **Gates** are **not** component parts of the system being analyzed. They are symbols representing the logic of the analysis. They are bi-modal. They function flawlessly.

Steps in Fault Tree Analysis



JACOBS SVERDRUP

Some Rules and Conventions

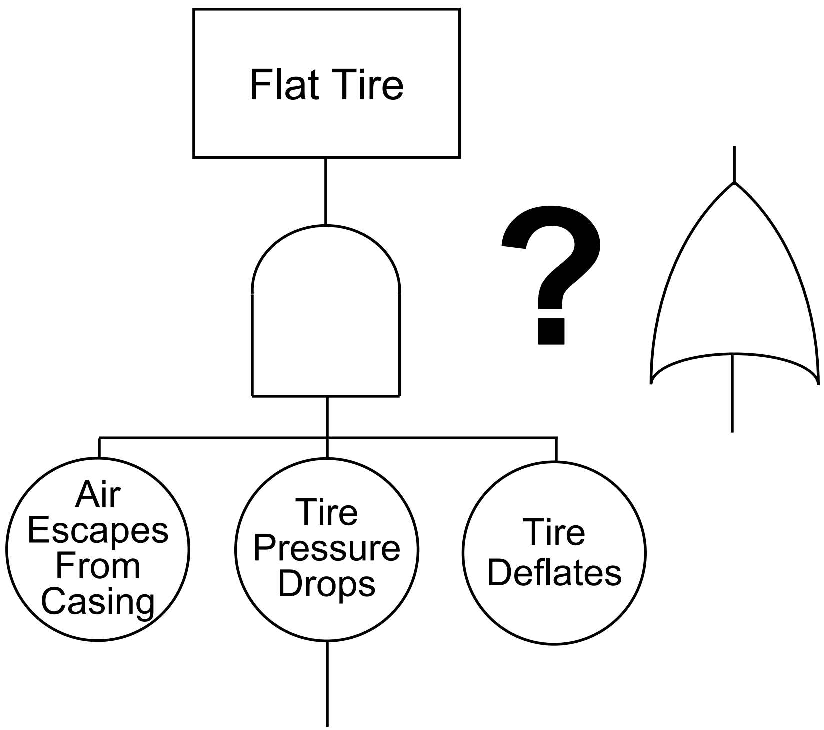


More Rules and Conventions

- Be CONSISTENT in naming fault events/conditions. Use same name for same event/condition throughout the analysis. (Use index numbering for large trees.)
- Say WHAT failed/faulted and HOW – e.g., “Switch Sw-418 contacts fail closed”
- Don’t expect **miracles** to “save” the system. Lightning will **not** recharge the battery. A large bass will **not** plug the hole in the hull.

JACOBS SVERDRUP

Some Conventions Illustrated



Initiators must be statistically independent of one another.
Name basics consistently!

- MAYBE
  - A gust of wind will come along and correct the skid.
  - A sudden cloudburst will extinguish the ignition source.
  - There'll be a power outage when the worker's hand contacts the high-voltage conductor.

No miracles!

JACOBS SVERDRUP

Identifying TOP Events

- Explore historical records (own and others).
- Look to energy sources.
- Identify potential mission failure contributors.
- Development "what-if" scenarios.
- Use "shopping lists."

JACOBS SVERDRUP

Example TOP Events

- Wheels-up landing
- Mid-air collision
- Subway derailment
- Turbine engine FOD
- Rocket failure to ignite
- Irretrievable loss of primary test data
- Dengue fever pandemic
- Sting failure
- Inadvertent nuke launch
- Reactor loss of cooling
- Uncommanded ignition
- Inability to dewater buoyancy tanks

TOP events represent potential high-penalty losses (i.e., high risk). Either severity of the outcome or frequency of occurrence can produce high risk.

JACOBS SVERDRUP

"Scope" the Tree TOP

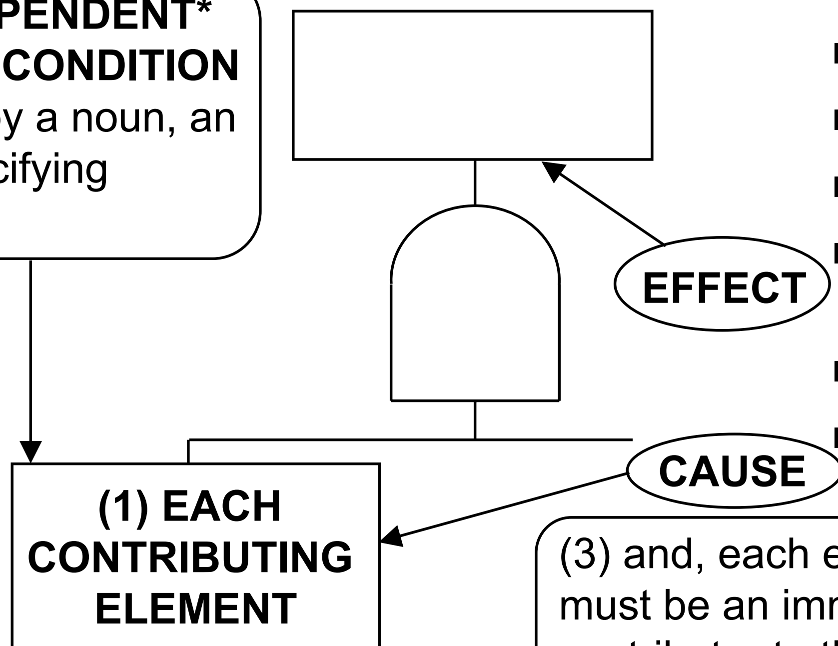
Too Broad	Improved
Computer Outage	Outage of Primary Data Collection computer, exceeding eight hours, from external causes
Exposed Conductor	Unprotected body contact with potential greater than 40 volts
Foreign Object Ingestion	Foreign object weighing more than 5 grams and having density greater than 3.2 gm/cc
Jet Fuel Dispensing Leak	Fuel dispensing fire resulting in loss exceeding $2,500

"Scoping" reduces effort spent in the analysis by confining it to relevant considerations. To "scope," describe the **level** of penalty or the **circumstances** for which the event becomes intolerable – use modifiers to narrow the event description.

Adding Contributors to the Tree

(2) must be an **INDEPENDENT* FAULT** or **FAILURE CONDITION** (typically described by a noun, an action verb, and specifying modifiers)

* At a given level, under a given gate, each fault must be independent of all others. However, the same fault may appear at other points on the tree.



(3) and, each element must be an immediate contributor to the level above

Examples:

- Electrical power fails off
- Low-temp. Alarm fails off
- Solar $\dot{q}$ > 0.043 btu/ft^2/ sec
- Relay K-28 contacts freeze closed
- Transducer case ruptures
- Proc. Step 42 omitted

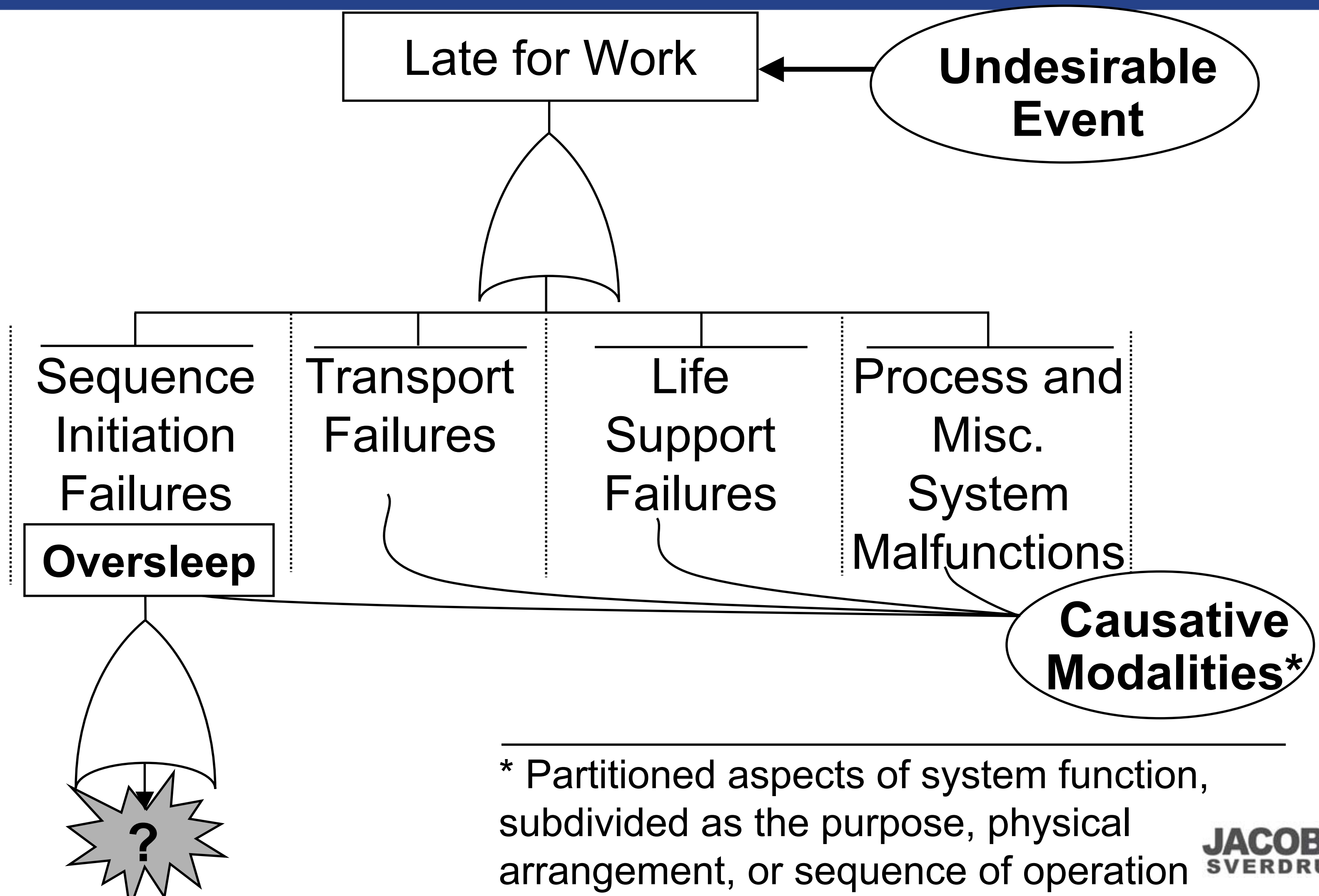
NOTE: As a **group** under an AND gate, and **individually** under an OR gate, contributing elements must be both **necessary** and **sufficient** to serve as **immediate** cause for the output event.

JACOBS SVERDRUP

Example Fault Tree Development

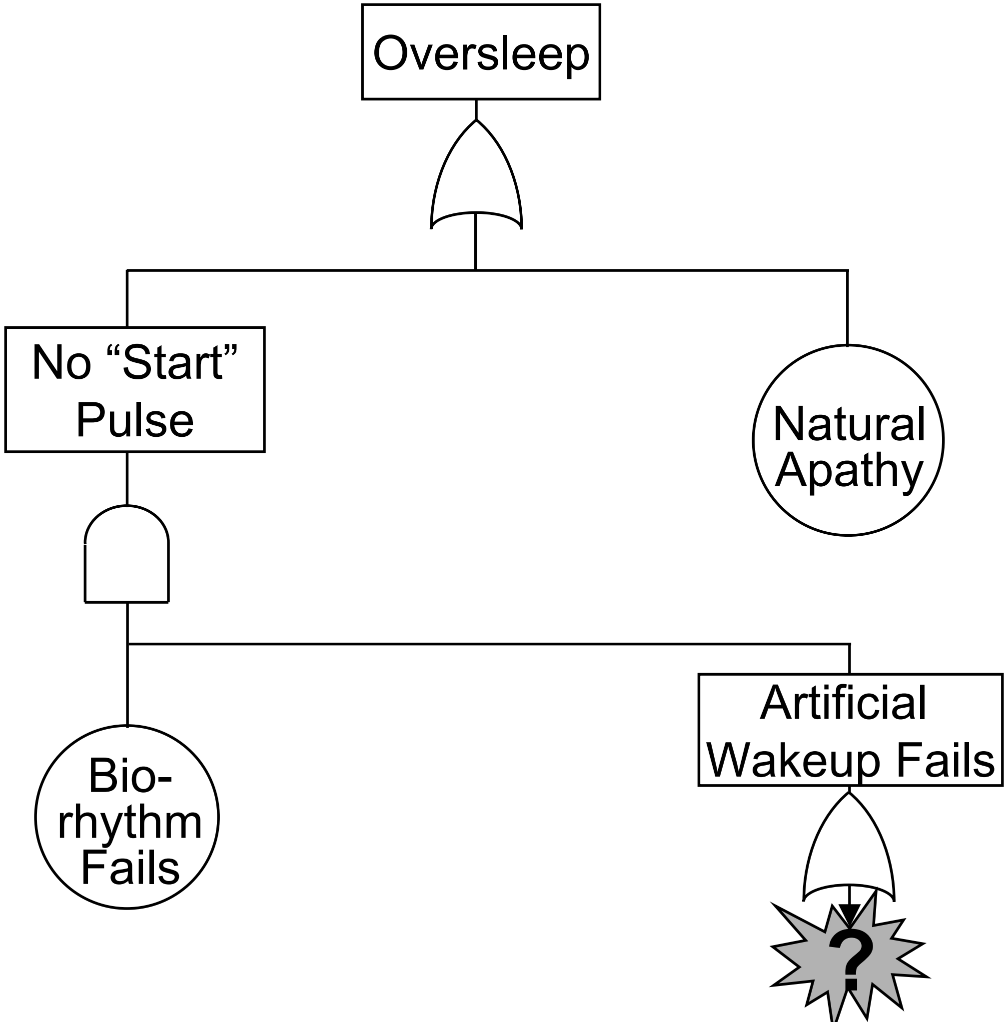
- Constructing the logic
- Spotting/correcting some common errors
- Adding quantitative data

An Example Fault Tree

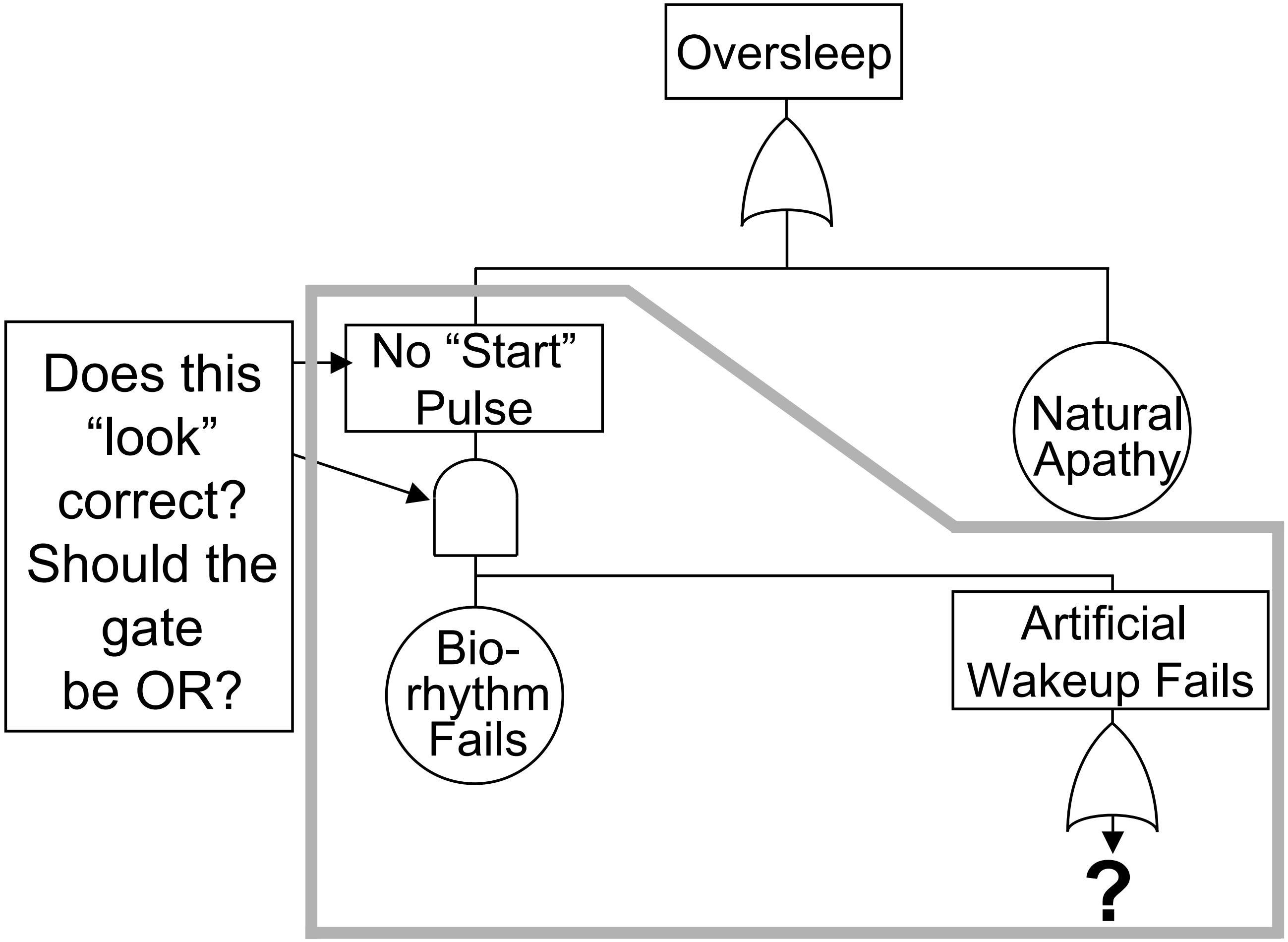


* Partitioned aspects of system function, subdivided as the purpose, physical arrangement, or sequence of operation

Sequence Initiation Failures

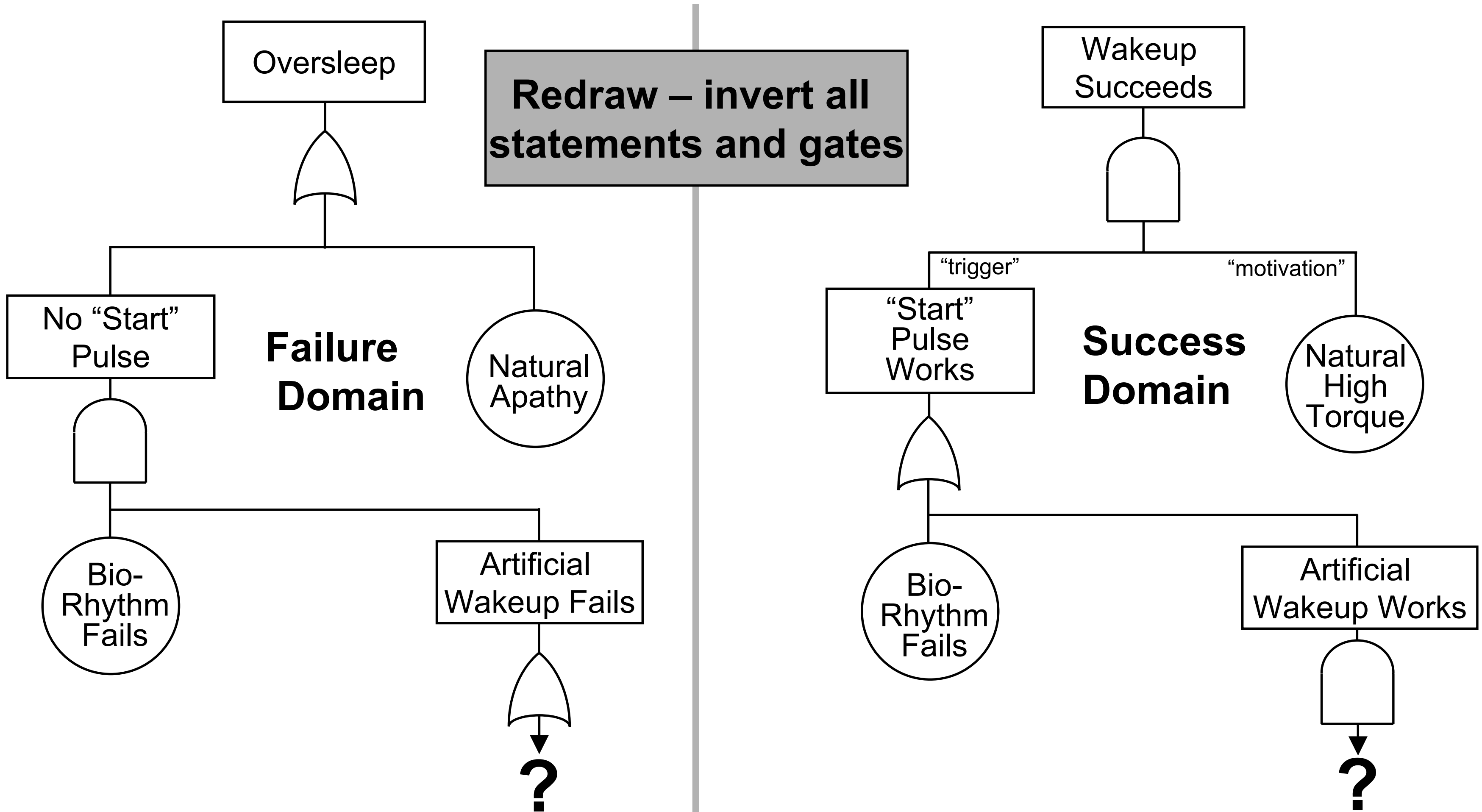


Verifying Logic



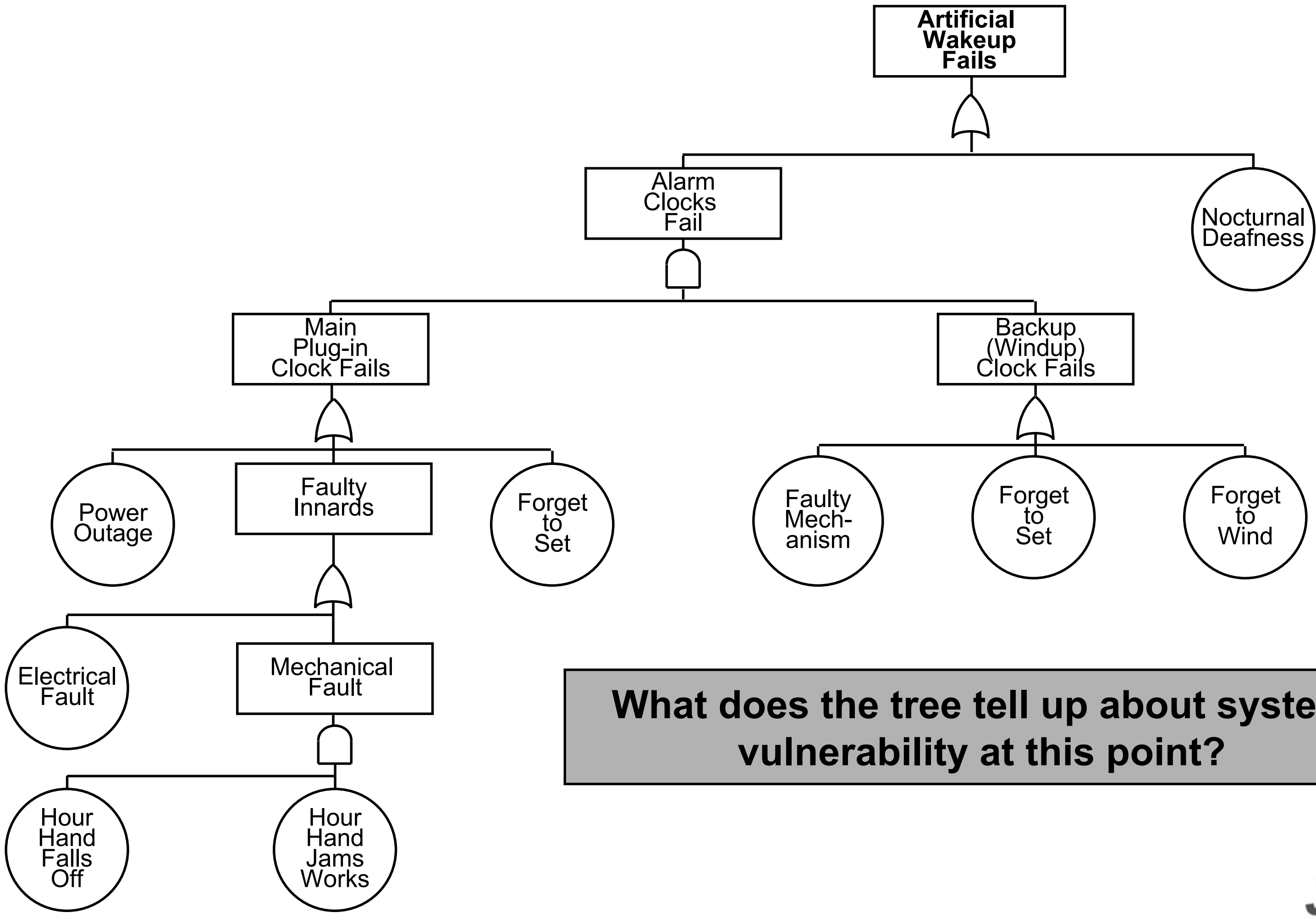
JACOBS SVERDRUP

Test Logic in SUCCESS Domain



If it was wrong here……it'll be wrong here, too!

Artificial Wakeup Fails



What does the tree tell up about system vulnerability at this point?

JACOBS SVERDRUP

Background for Numerical Methods

- Relating P_F to R
- The Bathtub Curve
- Exponential Failure Distribution
- Propagation through Gates
- P_F Sources

JACOBS SVERDRUP

Reliability and Failure Probability Relationships

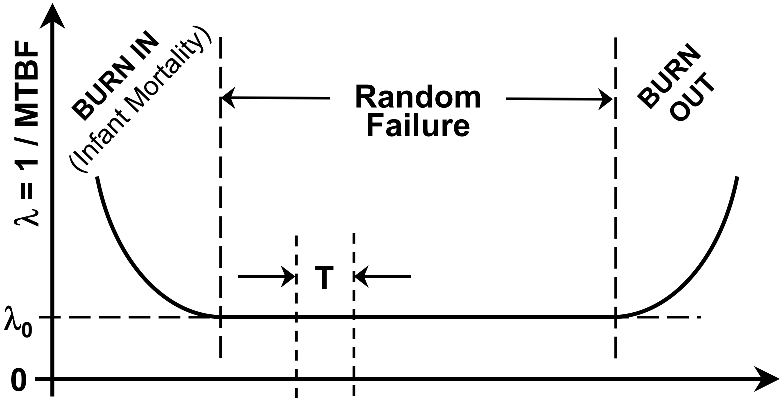
- S = Successes
- F = Failures
- Reliability… $R = \frac{S}{(S+F)}$
- Failure Probability… $P_F = \frac{F}{(S+F)}$

$$R + P_F = \frac{S}{(S+F)} + \frac{F}{(S+F)} \equiv 1$$

$$\lambda = \textbf{Fault Rate} = \frac{1}{\text{MTBF}}$$

JACOBS SVERDRUP

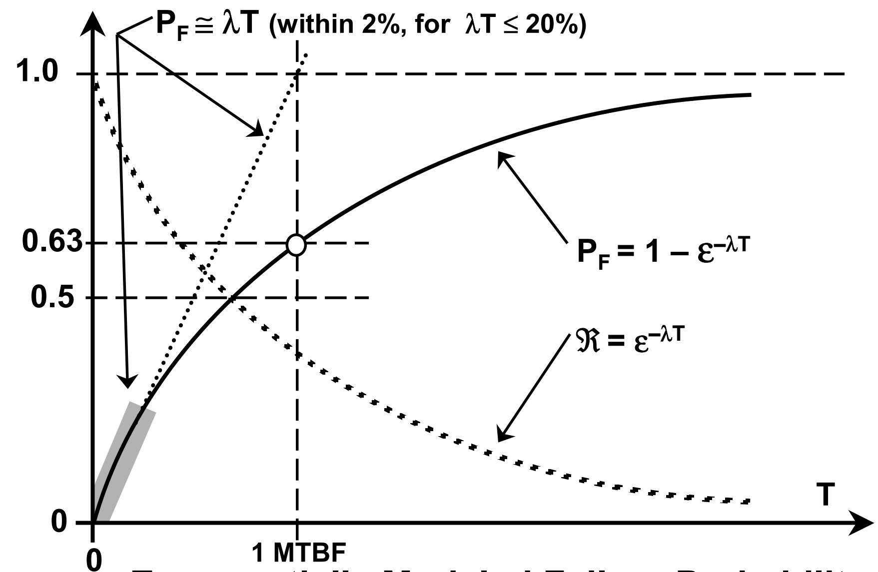
Significance of P_F



The Bathtub Curve

Most system elements have fault rates (λ = 1/MTBF) that are constant (λ_0) over long periods of useful life. During these periods, faults occur at random times.

Fault probability is modeled acceptably well as a function of exposure interval (T) by the exponential. For exposure intervals that are brief (T < 0.2 MTBF), P_F is approximated within 2% by λT.



Exponentially Modeled Failure Probability

JACOBS SVERDRUP

$\Re$ and P_F Through Gates

For 2 Inputs

OR Gate

Either of two, independent, element failures produces system failure.

$$\Re_T = \Re_A \Re_B$$

$P_F = 1 - \Re_T$

$P_F = 1 \ (\Re_A \Re_B)$

$P_F = 1 - [(1 - P_A)(1 - P_B)]$

$$\mathbf{P_F = P_A + P_B - P_A P_B}$$ **[Union / $\cup$]**

…for $P_{A,B} \leq 0.2$
$\mathbf{P_F \cong P_A + P_B}$
with error $\leq$ 11%

← **"Rare Event Approximation"**

AND Gate

Both of two, independent elements must fail to produce system failure.

$$\Re_T = \Re_A + \Re_B - \Re_A \Re_B$$

$P_F = 1 - \Re_T$

$P_F = 1 - (\Re_A + \Re_B - \Re_A \Re_B)$

$P_F = 1 - [(1 - P_A) + (1 - P_B) - (1 - P_A)(1 - P_B)]$

$$\mathbf{P_F = P_A P_B}$$ **[Intersection / $\cap$]**

$R + P_F \equiv 1$

For 3 Inputs

OR Gate:

$$\mathbf{P_F = P_A + P_B + P_C}$$

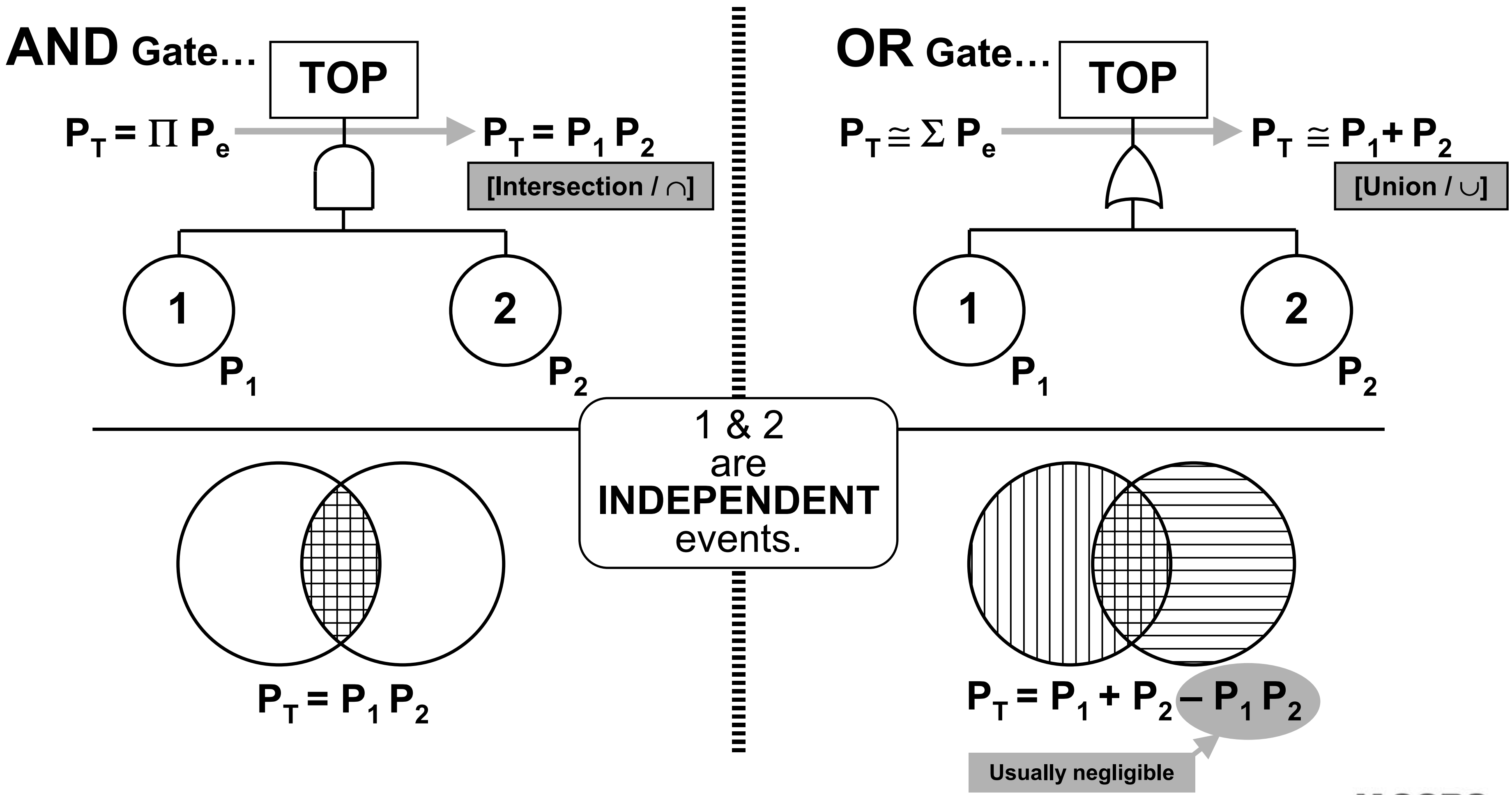
$- P_A P_B - P_A P_C - P_B P_C$
$+ P_A P_B P_C$

← **Omit for approximation**

AND Gate:

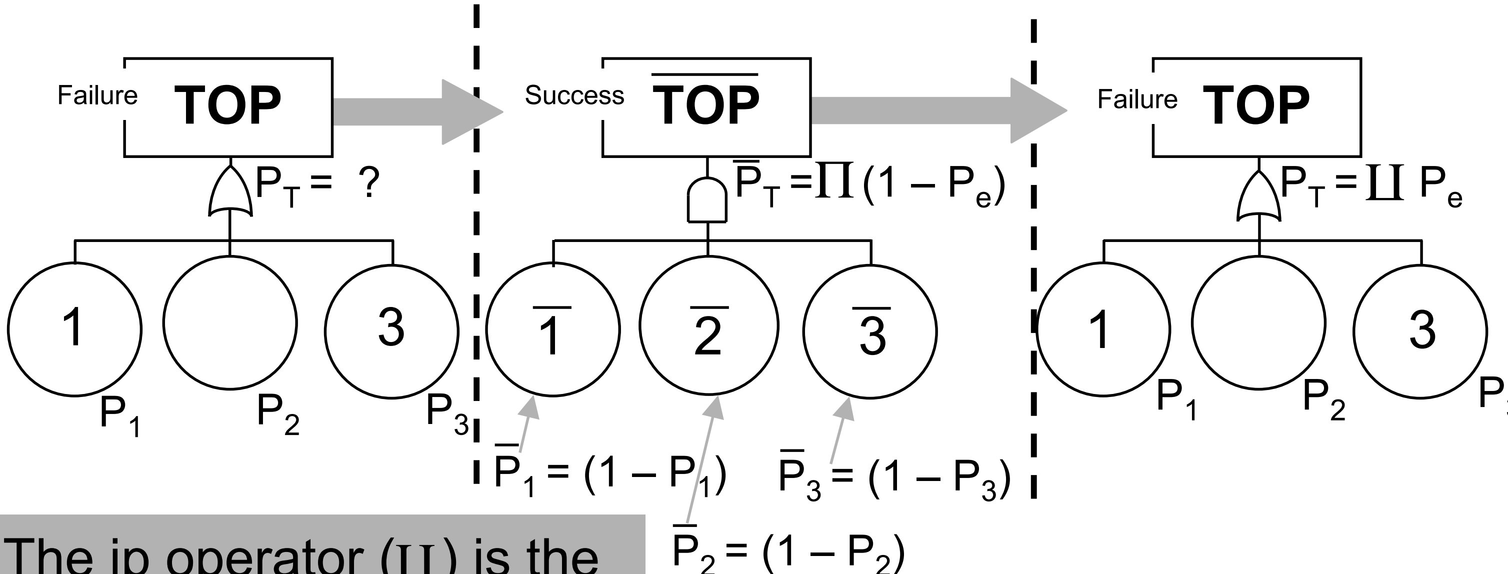
$$\mathbf{P_F = P_A P_B P_C}$$

P_F Propagation Through Gates



JACOBS SVERDRUP

"Ipping" Gives Exact OR Gate Solutions



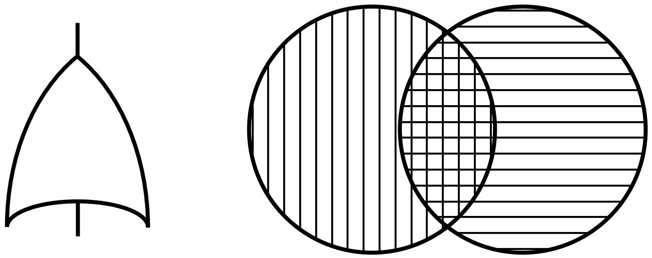
The ip operator ($\coprod$) is the co-function of pi ($\prod$). It provides an exact solution for propagating probabilities through the **OR** gate. Its use is rarely justifiable.

$$P_T = \coprod P_e = 1 - \prod (1 - P_e)$$

$$P_T = 1 - [(1 - P_1)\ (1 - P_2)\ (1 - P_3\ \ldots\ (1 - P_n)]$$

JACOBS SVERDRUP

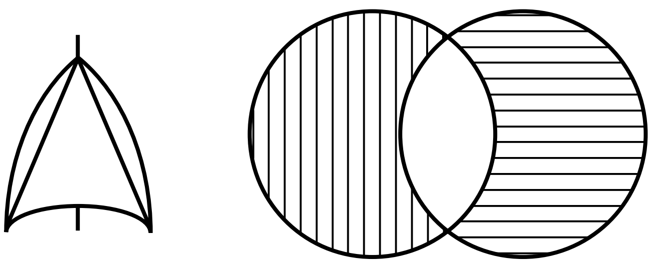
More Gates and Symbols



Inclusive OR Gate…

$\mathbf{P_T = P_1 + P_2 - (P_1 \times P_2)}$

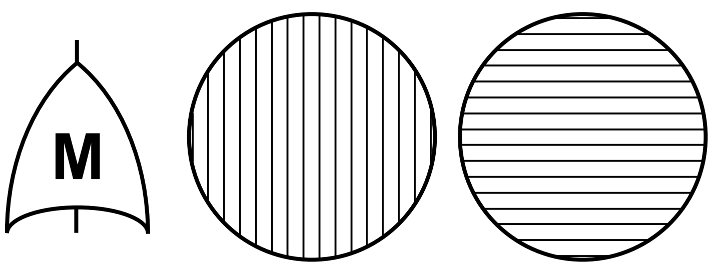
Opens when any *one or more* events occur.



Exclusive OR Gate…

$\mathbf{P_T = P_1 + P_2 - 2\,(P_1 \times P_2)}$

Opens when any one (but *only* one) event occurs.



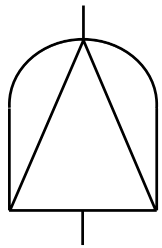
Mutually Exclusive OR Gate…

$\mathbf{P_T = P_1 + P_2}$

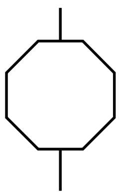
Opens when any one of two or more events occur. All other events are then *precluded*.

For *all* **OR** Gate cases, the Rare Event Approximation may be used for small values of P_e. $\mathbf{P_T \cong \Sigma P_e}$

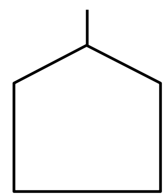
Still More Gates and Symbols



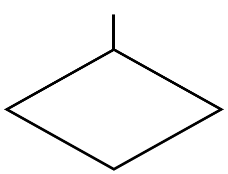
Priority AND Gate
$P_T = P_1 \times P_2$
Opens when input events occur in predetermined sequence.



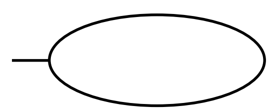
Inhibit Gate
Opens when (single) input event occurs in presence of enabling condition.



External Event
An event normally expected to occur.



Undeveloped Event
An event not further developed.



Conditioning Event
Applies conditions or restrictions to other symbols.

JACOBS SVERDRUP

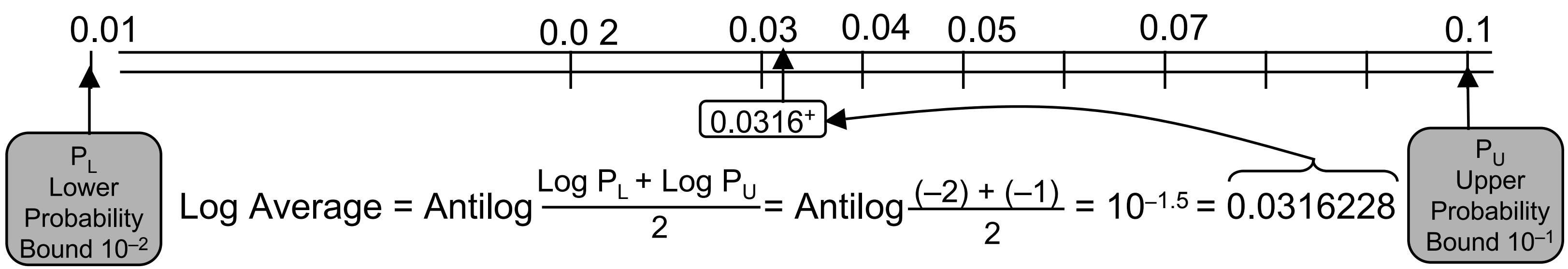
Some Failure Probability Sources

- Manufacturer's Data
- Industry Consensus Standards
- MIL Standards
- Historical Evidence – Same or Similar Systems
- Simulation/testing
- Delphi Estimates
- ERDA Log Average Method

Log Average Method*

If probability is not estimated easily, but upper and lower credible bounds can be judged…

- Estimate upper and lower credible bounds of probability for the phenomenon in question.
- Average the logarithms of the upper and lower bounds.
- The antilogarithm of the average of the logarithms of the upper and lower bounds is less than the upper bound and greater than the lower bound by the same factor. Thus, it is geometrically midway between the limits of estimation.



$$\text{Log Average} = \text{Antilog}\,\frac{\text{Log } P_L + \text{Log } P_U}{2} = \text{Antilog}\,\frac{(-2)+(-1)}{2} = 10^{-1.5} = 0.0316228$$

Note that, for the example shown, the arithmetic average would be…

$$\frac{0.01 + 0.1}{2} = 0.055$$

i.e., 5.5 times the lower bound and 0.55 times the upper bound

* Reference: Briscoe, Glen J.; “Risk Management Guide;” System Safety Development Center; SSDC-11; DOE 76-45/11; September 1982.

JACOBS SVERDRUP

More Failure Probability Sources

- WASH-1400 (NUREG-75/014); “Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants;” 1975
- IEEE Standard 500
- Government-Industry Data Exchange Program (GIDEP)
- Rome Air Development Center Tables
- NUREG-0492; “Fault Tree Handbook;” (Table XI-1); 1986
- Many others, including numerous industry-specific proprietary listings

JACOBS SVERDRUP

Typical Component Failure Rates

	Failures Per 10^6 Hours		
Device	**Minimum**	**Average**	**Maximum**
Semiconductor Diodes	0.10	1.0	10.0
Transistors	0.10	3.0	12.0
Microwave Diodes	3.0	10.0	22.0
MIL-R-11 Resistors	0.0035	0.0048	0.016
MIL-R-22097 Resistors	29.0	41.0	80.0
Rotary Electrical Motors	0.60	5.0	500.0
Connectors	0.01	0.10	10.0

Source: Willie Hammer, “Handbook of System and Product Safety,” Prentice Hall

JACOBS SVERDRUP

Typical Human Operator Failure Rates

Activity	Error Rate
*Error of omission/item embedded in procedure	3×10^{-3}
*Simple arithmetic error with self-checking	3×10^{-2}
*Inspector error of operator oversight	10^{-1}
*General rate/high stress/ dangerous activity	0.2-0.3
**Checkoff provision improperly used	0.1-0.09 (0.5 avg.)
**Error of omission/10-item checkoff list	0.0001-0.005 (0.001 avg.)
**Carry out plant policy/no check on operator	0.005-0.05 (0.01 avg.)
**Select wrong control/group of identical, labeled, controls	0.001-0.01 (0.003 avg.)

Sources: * WASH-1400 (NUREG-75/014); "Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," 1975
**NUREG/CR-1278; "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," 1980

JACOBS SVERDRUP

Some Factors Influencing Human Operator Failure Probability

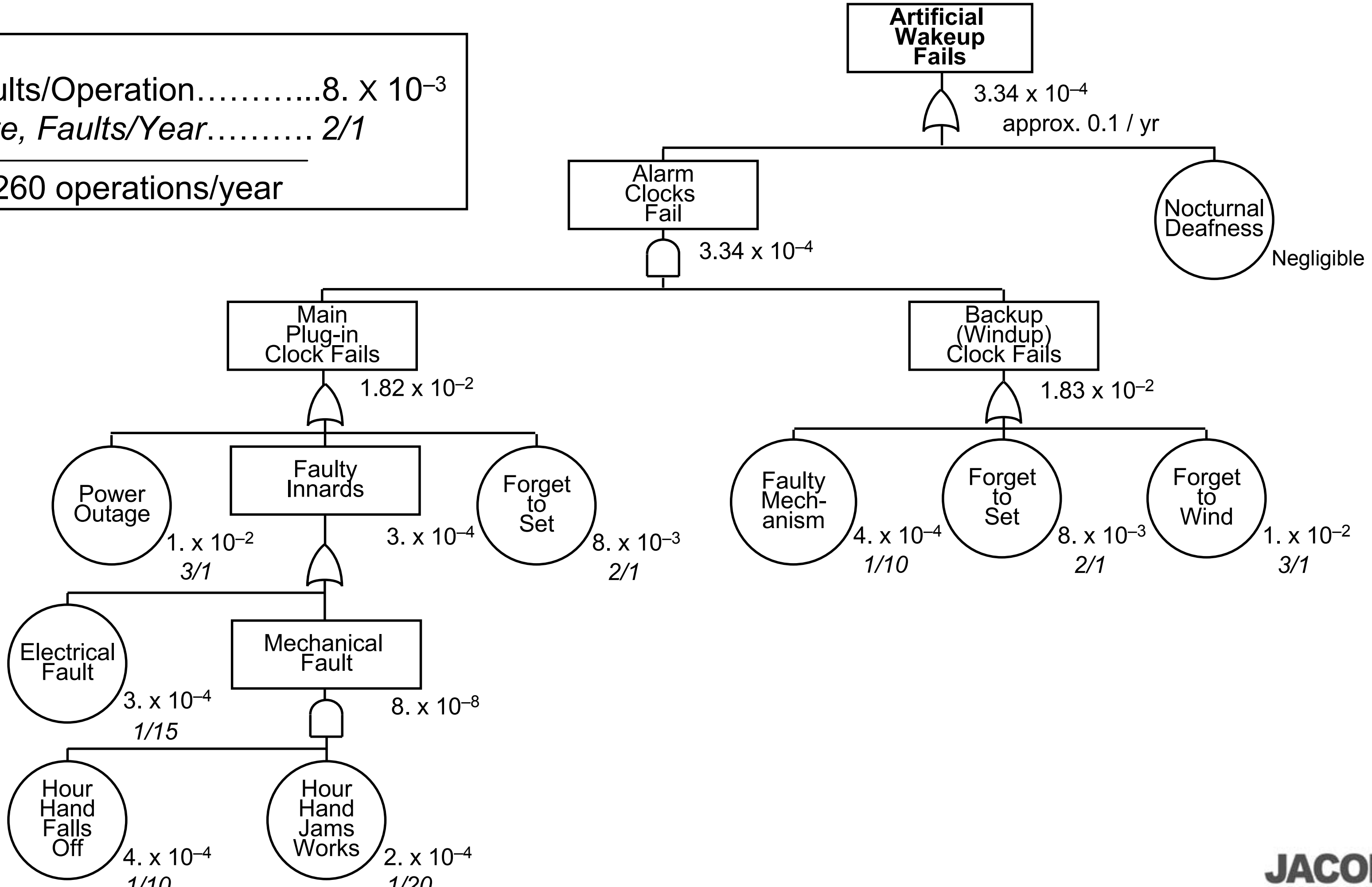
- Experience
- Stress
- Training
- Individual self discipline/conscientiousness
- Fatigue
- Perception of error consequences (…to self/others)
- Use of guides and checklists
- Realization of failure on prior attempt
- Character of Task – Complexity/Repetitiveness

JACOBS SVERDRUP

Artificial Wakeup Fails

KEY: Faults/Operation………...8. X 10^{-3}
Rate, Faults/Year………. 2/1

Assume 260 operations/year



JACOBS SVERDRUP

HOW Much P_T is TOO Much?

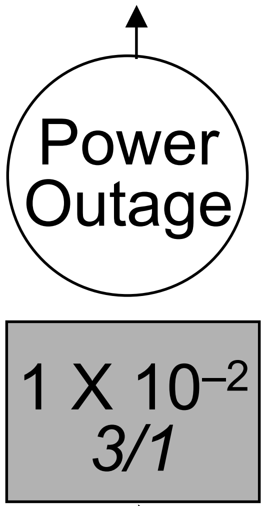
Consider "bootstrapping" comparisons with known risks…

Human operator error (response to repetitive stimulus)	$\cong 10^{-2}$- 10^{-3}/exp MH†
Internal combustion engine failure (spark ignition)	$\cong 10^{-3}$/exp hr†
Pneumatic instrument recorder failure	$\cong 10^{-4}$/exp hr†
Distribution transformer failure	$\cong 10^{-5}$/exp hr†
U.S. Motor vehicles fatalities	$\cong 10^{-6}$/exp MH†
Death by disease (U.S. lifetime avg.)	$\cong 10^{-6}$/exp MH
U.S. Employment fatalities	$\cong 10^{-7}$-10^{-8}/exp MH†
Death by lightning	$\cong 10^{-9}$/exp MH*
Meteorite (>1 lb) hit on 10^3x 10^3 ft area of U.S.	$\cong 10^{-10}$/exp hr‡
Earth destroyed by extraterrestrial hit	$\cong 10^{-14}$/exp hr†

† Browning, R.L., "The Loss Rate Concept in Safety Engineering"
* National Safety Council, "Accident Facts"
‡ Kopecek, J.T., "Analytical Methods Applicable to Risk Assessment & Prevention," Tenth International System Safety Conference

JACOBS SVERDRUP

Apply Scoping



What power outages are of **concern**?

Not all of them!

Only those that…

- Are undetected/uncompensated
- Occur during the hours of sleep
- Have sufficient duration to fault the system

This probability must reflect these conditions!

JACOBS SVERDRUP

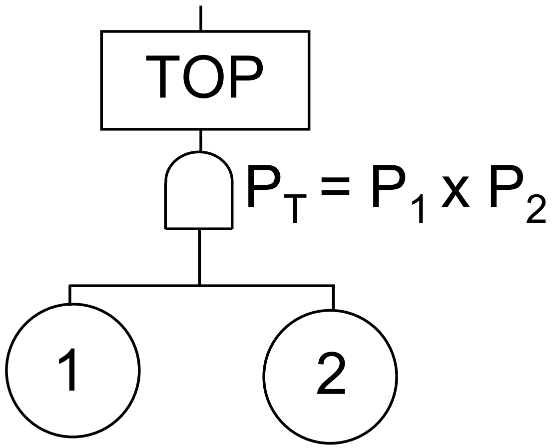
Single-Point Failure

"A failure of ***one independent element*** of a system which causes an ***immediate*** hazard to occur and/or causes the whole system to fail."

Professional Safety – March 1980

JACOBS SVERDRUP

Some AND Gate Properties

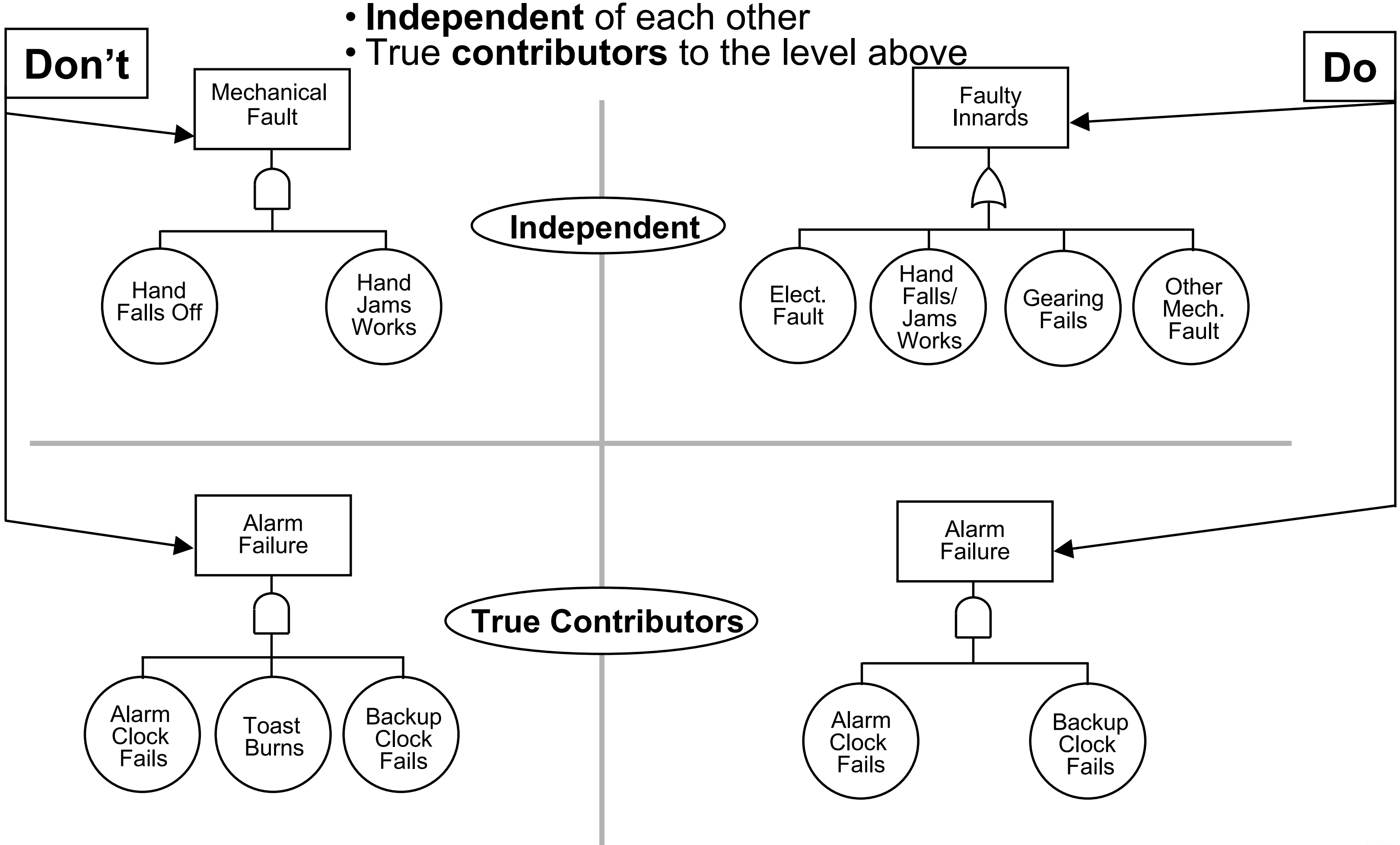


Cost:
Assume two identical elements having P = 0.1.
$P_T = 0.01$
Two elements having P = 0.1 may cost much less than one element having P = 0.01.

Freedom from single point failure:
Redundancy ensures that either 1 or 2 may fail without inducing TOP.

Failures at Any Analysis Level Must Be

- **Independent** of each other
- True **contributors** to the level above



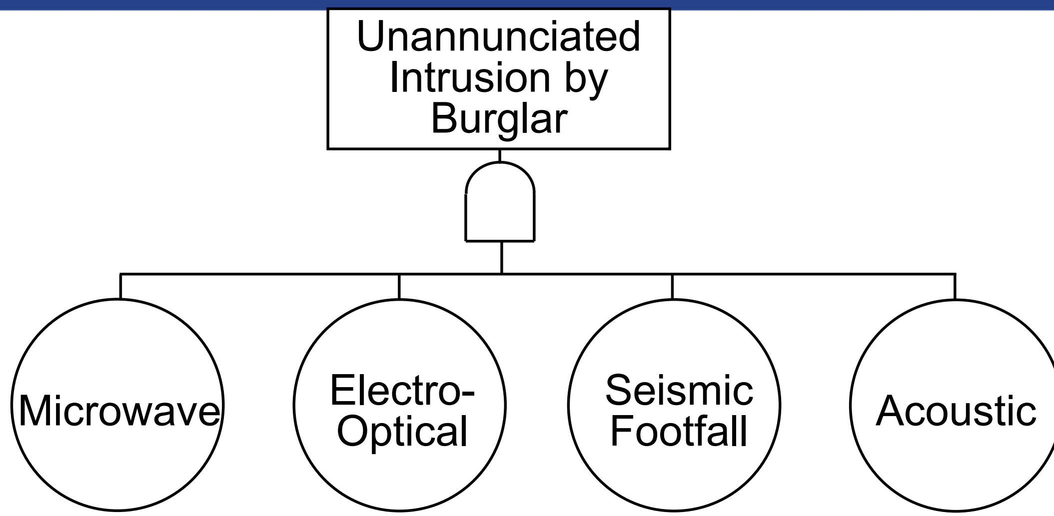
JACOBS SVERDRUP

Common Cause Events/Phenomena

"A Common Cause is an event or a phenomenon which, if it occurs, will induce the occurrence of two or more fault tree elements."

Oversight of Common Causes is a frequently found fault tree flaw!

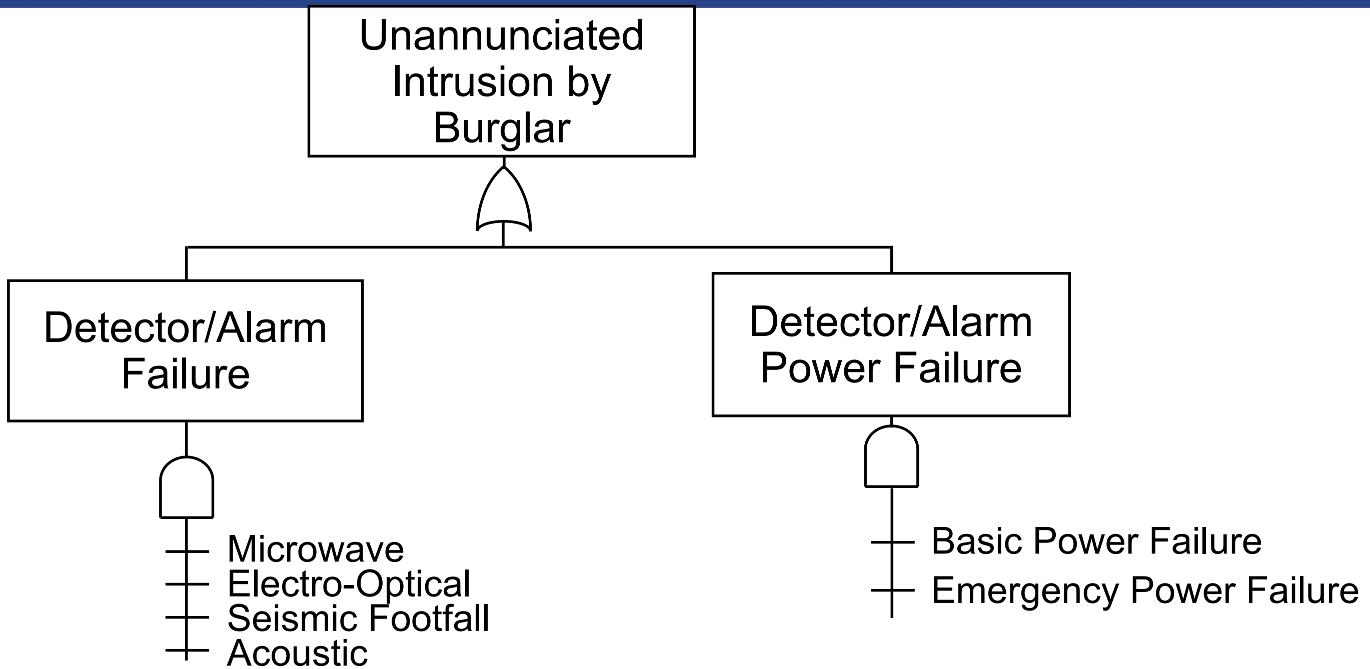
Common Cause Oversight – An Example



DETECTOR/ALARM FAILURES

Four, wholly independent alarm systems are provided to detect and annunciate intrusion. No two of them share a common operating principle. Redundancy appears to be absolute. The AND gate to the TOP event seems appropriate. But, suppose the four systems share a single source of operating power, and that source fails, and there are no backup sources?

Common Cause Oversight Correction



Here, power source failure has been recognized as an event which, if it occurs, will disable all four alarm systems. Power failure has been accounted for as a common cause event, leading to the TOP event through an OR gate. **OTHER COMMON CAUSES SHOULD ALSO BE SEARCHED FOR.**

Example Common Cause Fault/Failure Sources

- Utility Outage
  - Electricity
  - Cooling Water
  - Pneumatic Pressure
  - Steam
- Moisture
- Corrosion
- Seismic Disturbance
- Dust/Grit
- Temperature Effects (Freezing/Overheat)
- Electromagnetic Disturbance
- Single Operator Oversight
- Many Others

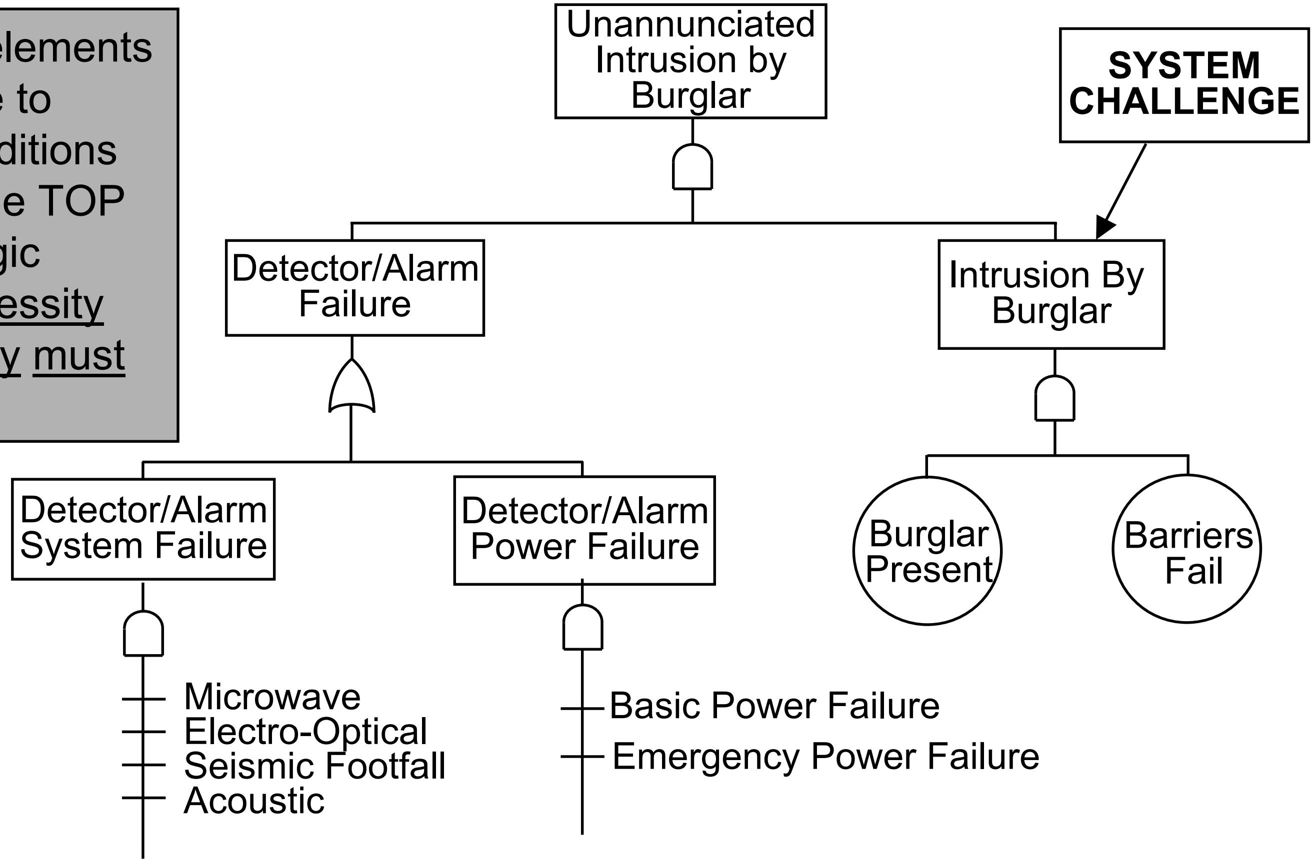
Example Common Cause Suppression Methods

- Separation/Isolation/Insulation/Sealing/ Shielding of System Elements.
- Using redundant elements having differing operating principles.
- Separately powering/servicing/maintaining redundant elements.
- Using independent operators/inspectors.

JACOBS SVERDRUP

Missing Elements?

Contributing elements must combine to satisfy all conditions essential to the TOP event. The logic criteria of necessity and sufficiency must be satisfied.

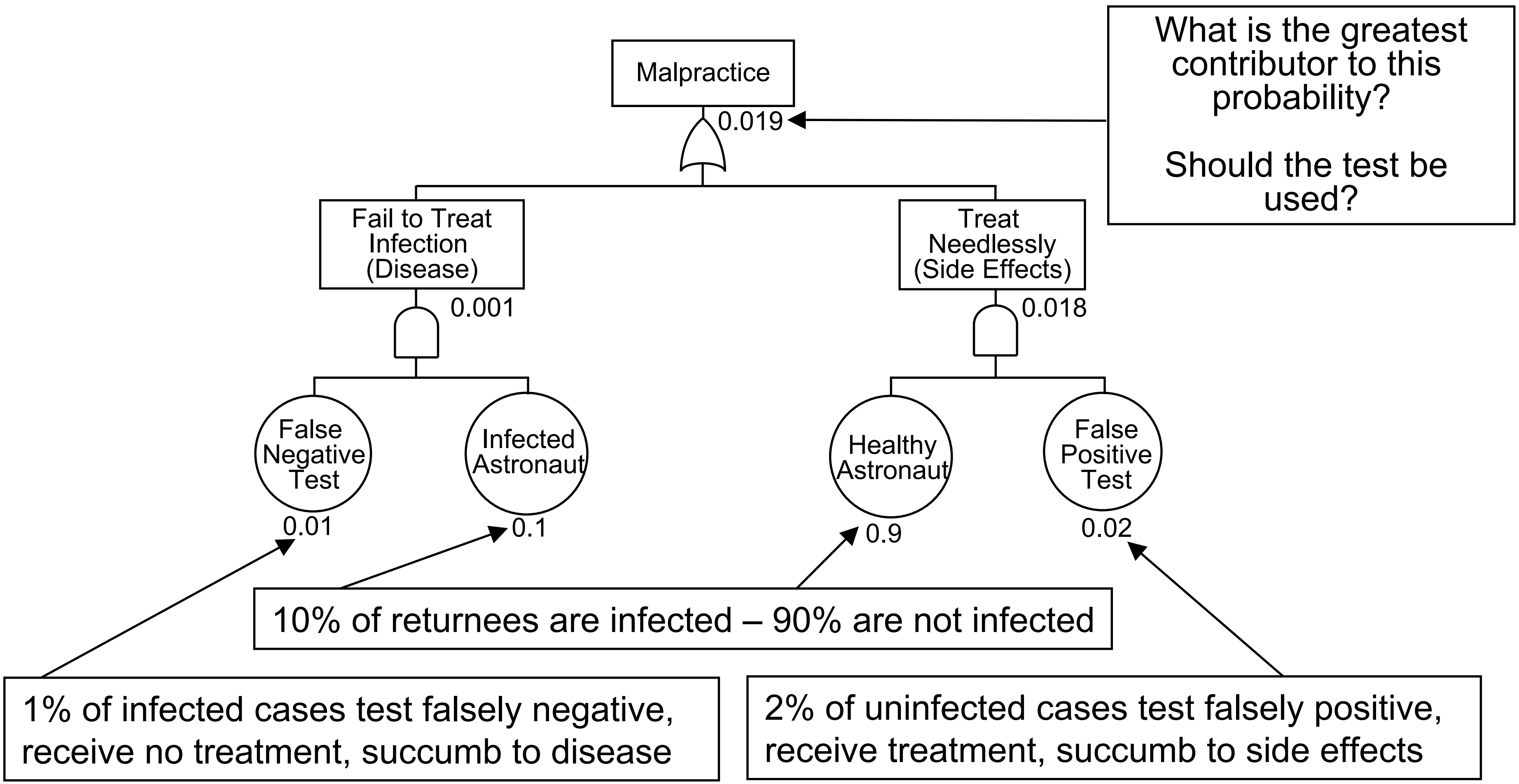


Example Problem – Sclerotic Scurvy – The Astronaut's Scourge

- **BACKGROUND:** Sclerotic scurvy infects 10% of all returning astronauts. Incubation period is 13 days. For a week thereafter, victims of the disease display symptoms which include malaise, lassitude, and a very crabby outlook. A test can be used during the incubation period to determine whether an astronaut has been infected. Anti-toxin administered during the incubation period is 100% effective in preventing the disease when administered to an infected astronaut. However, for an uninfected astronaut, it produces disorientation, confusion, and intensifies all undesirable personality traits for about seven days. The test for infection produces a false positive result in 2% of all uninfected astronauts and a false negative result in one percent of all infected astronauts. Both treatment of an uninfected astronaut and failure to treat an infected astronaut constitute in malpractice.
- **Problem:** Using the test for infection and the anti-toxin, if the test indicates need for it, what is the probability that a returning astronaut will be a victim of malpractice?

JACOBS SVERDRUP

Sclerotic Scurvy Malpractice



JACOBS SVERDRUP

Cut Sets

AIDS TO…

- System Diagnosis
- Reducing Vulnerability
- Linking to Success Domain

- A **CUT SET** is *any* group of fault tree initiators which, if all occur, will cause the TOP event to occur.
- A **MINIMAL CUT SET** is a *least* group of fault tree initiators which, if all occur, will cause the TOP event to occur.

JACOBS SVERDRUP

Finding Cut Sets

1. Ignore all tree elements except the initiators ("leaves/basics").
2. Starting immediately below the TOP event, assign a unique letter to each gate, and assign a unique number to each initiator.
3. Proceeding stepwise from TOP event downward, construct a matrix using the letters and numbers. The letter representing the TOP event gate becomes the initial matrix entry. As the construction progresses:
   - Replace the letter for each AND gate by the letter(s)/number(s) for all gates/initiators which are its inputs. Display these horizontally, in matrix rows.
   - Replace the letter for each OR gate by the letter(s)/number(s) for all gates/initiators which are its inputs. Display these vertically, in matrix columns. Each newly formed OR gate replacement row must also contain all other entries found in the original parent row.

JACOBS SVERDRUP

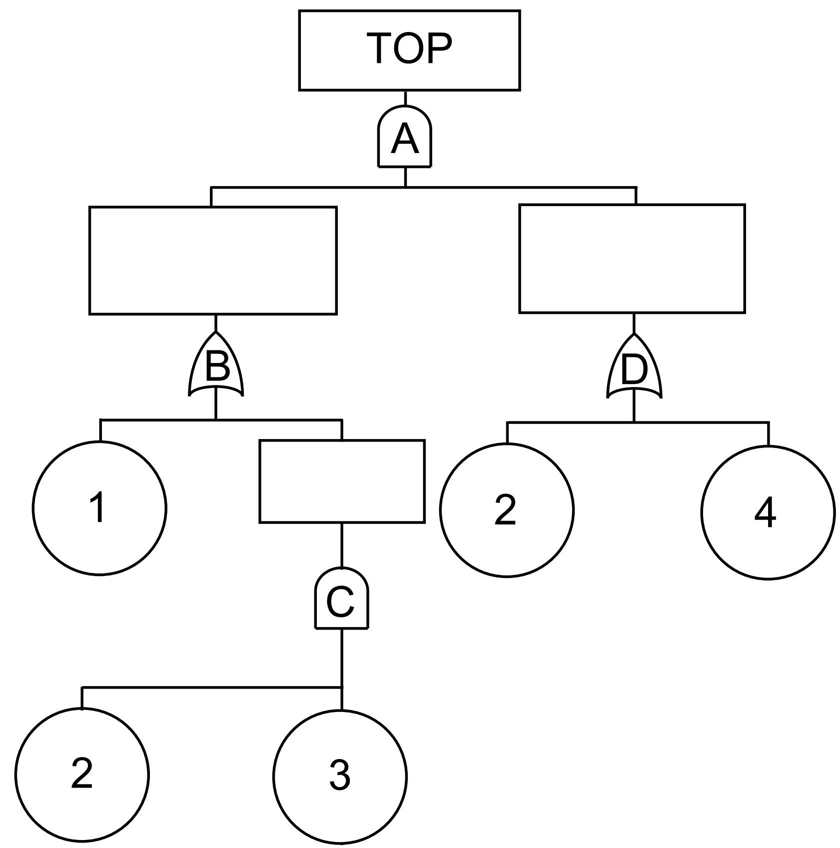
Finding Cut Sets

4. A final matrix results, displaying only numbers representing initiators. Each row of this matrix is a Boolean Indicated Cut Set. By inspection, eliminate any row that contains all elements found in a lesser row. Also eliminate redundant elements within rows and rows that duplicate other rows. The rows that remain are Minimal Cut Sets.

JACOBS SVERDRUP

A Cut Set Example

- **PROCEDURE:**
  - Assign letters to gates. (TOP gate is “A.”) Do not repeat letters.
  - Assign numbers to basic initiators. If a basic initiator appears more than once, represent it by the same number at each appearance.
  - Construct a matrix, starting with the TOP “A” gate.



A Cut Set Example

A		

TOP event gate is **A**, the initial matrix entry.

B	D	

A is an AND gate; **B** & **D**, its inputs, replace it horizontally.

1	D	
C	D	

B is an OR gate; **1** & **C**, its inputs, replace it vertically. Each requires a new row.

1	D	
2	D	3

C is an AND gate; **2** & **3**, its inputs, replace it horizontally.

1	2	
2	D	3
1	4	

D (top row), is an OR gate; **2** & **4**, its inputs, replace it vertically. Each requires a new row.

1	2	
2	2	3
1	4	
2	4	3

D (second row), is an OR gate. Replace as before.

These Boolean-Indicated Cut Sets…

…reduce to these minimal cut sets.

1	**2**
2	**3**
1	**4**

Minimal Cut Set rows are least groups of initiators which will induce TOP.

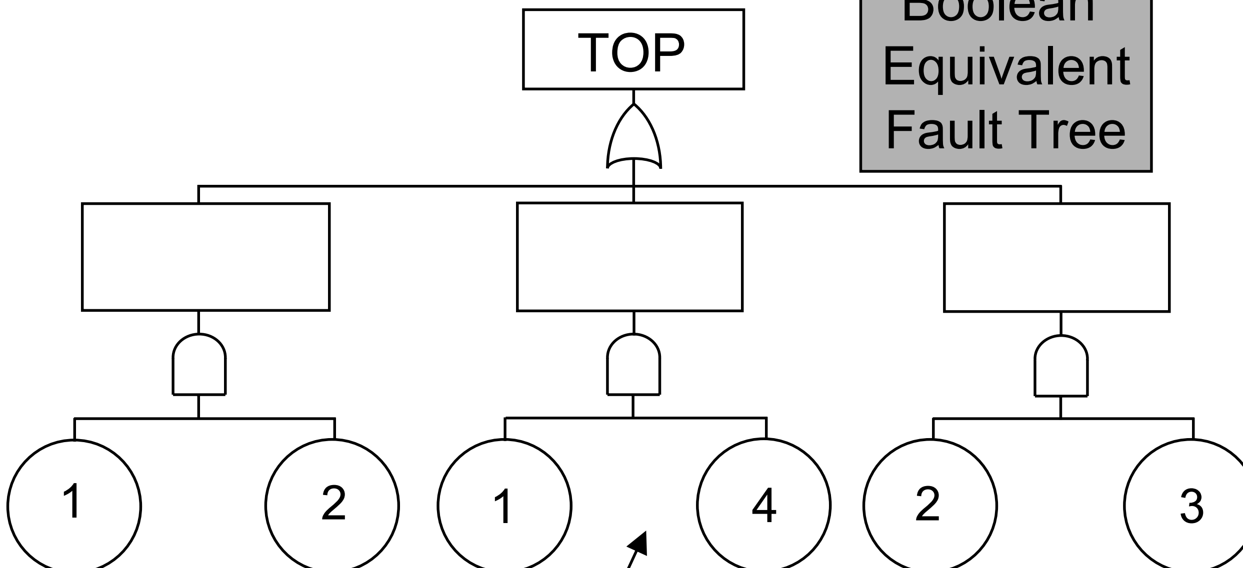
JACOBS SVERDRUP

An "Equivalent" Fault Tree

Boolean Equivalent Fault Tree

An Equivalent Fault Tree can be constructed from Minimal Cut Sets. For example, these Minimal Cut Sets…

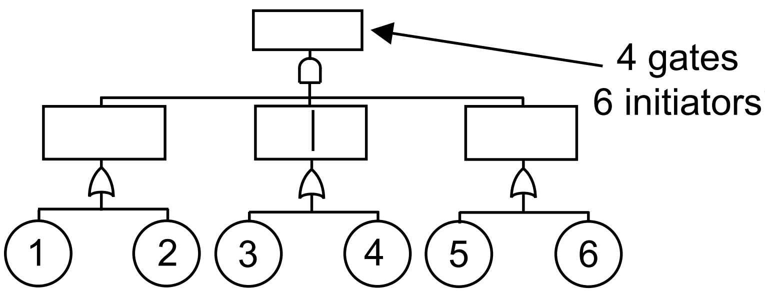
1	2
2	3
1	4



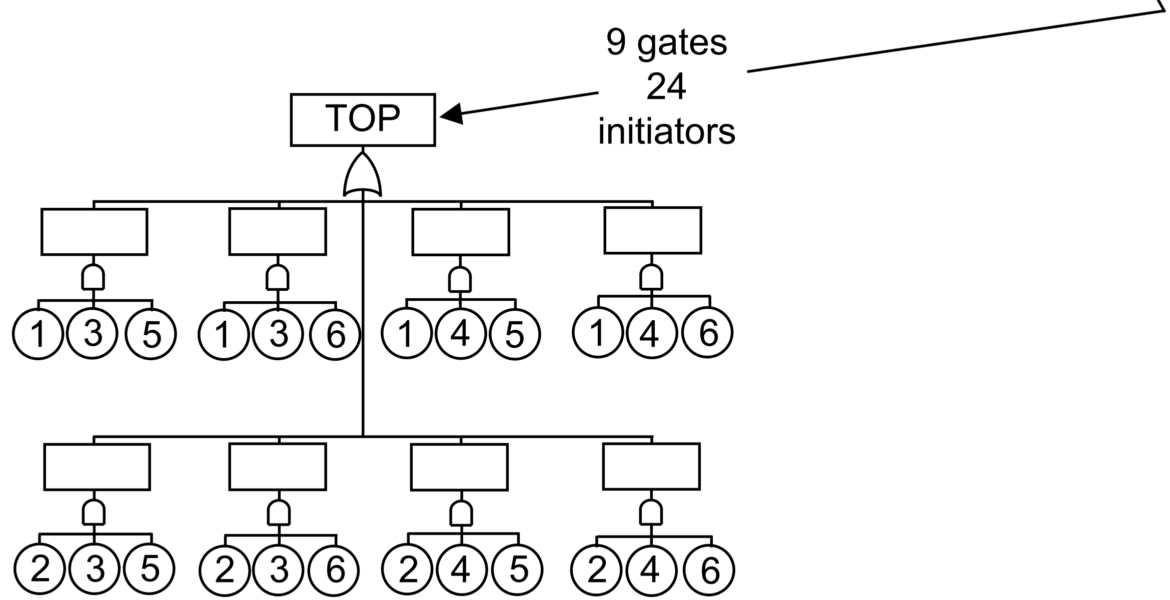
…represent this Fault Tree…

…and this Fault Tree is a Logic Equivalent of the original, for which the Minimal Cut Sets were derived.

Equivalent Trees Aren't Always Simpler



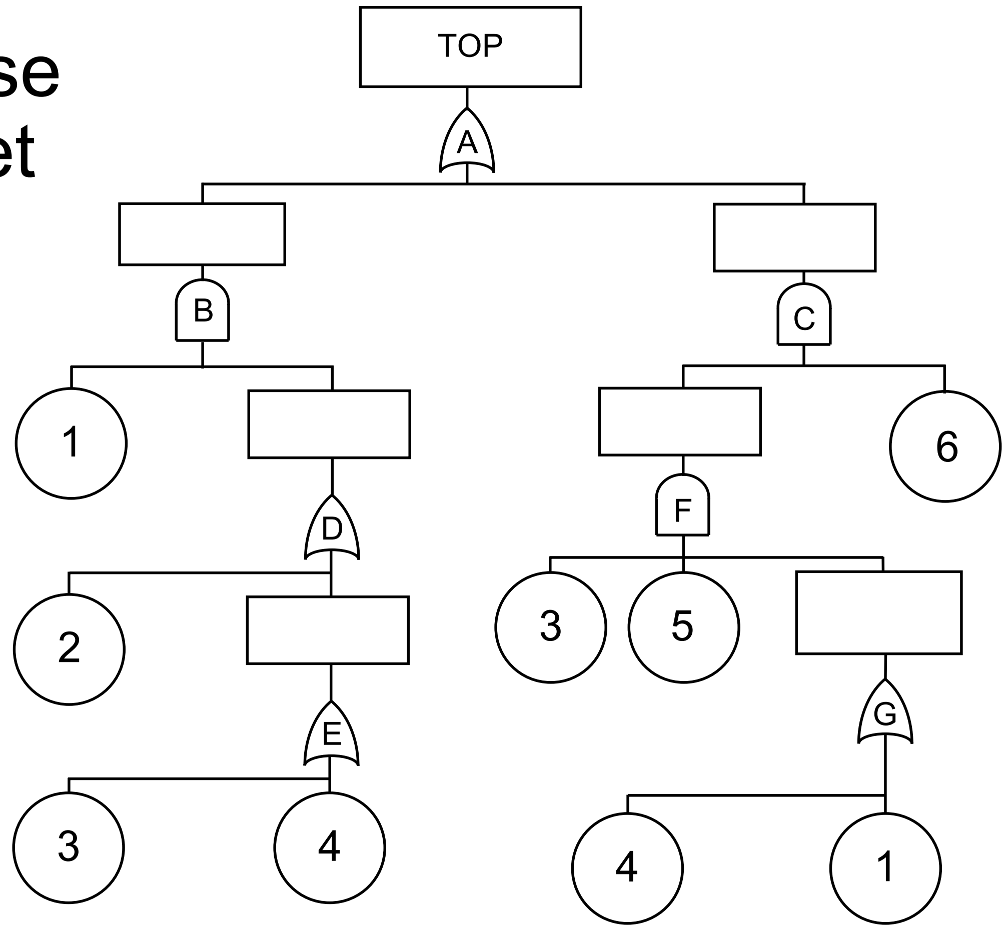
This Fault Tree has this logic equivalent.



Minimal cut sets
1/3/5
1/3/6
1/4/5
1/4/6
2/3/5
2/3/6
2/4/5
2/4/6

Another Cut Set Example

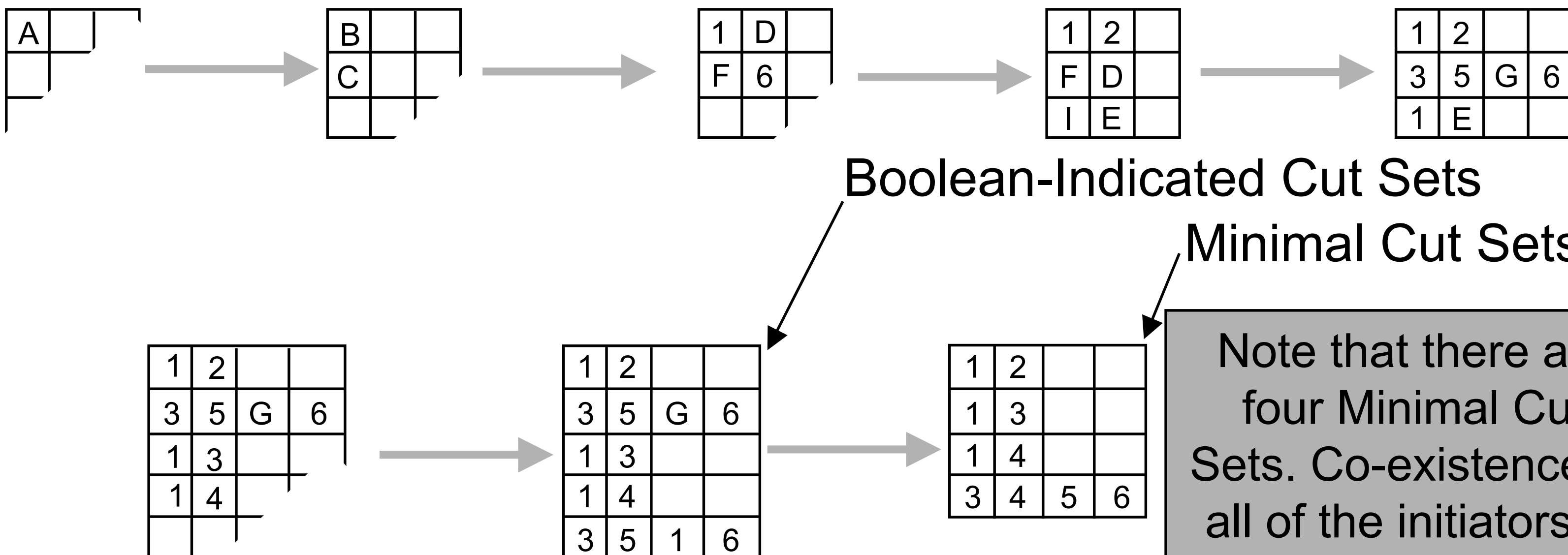
- Compare this case to the first Cut Set example – note differences. TOP gate here is OR. In the first example, TOP gate was AND.
- Proceed as with first example.



JACOBS SVERDRUP

Another Cut Set Example

Construct Matrix – make step-by-step substitutions…



Note that there are four Minimal Cut Sets. Co-existence of all of the initiators in any one of them will precipitate the TOP event.

An **EQUIVALENT FAULT TREE** can again be constructed…

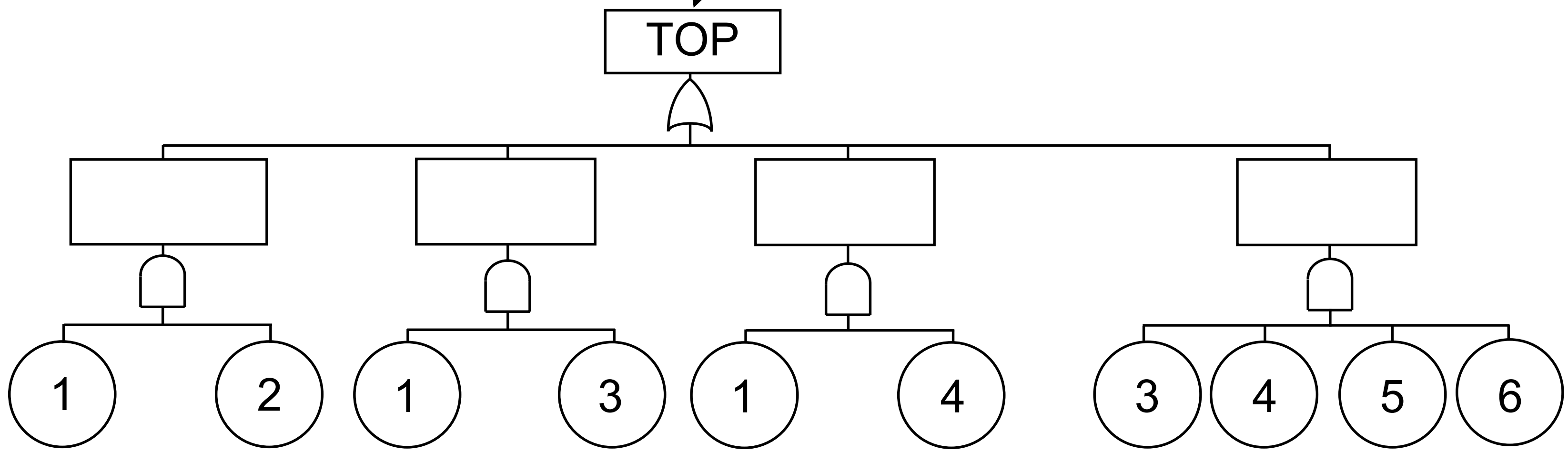
JACOBS SVERDRUP

Another "Equivalent" Fault Tree

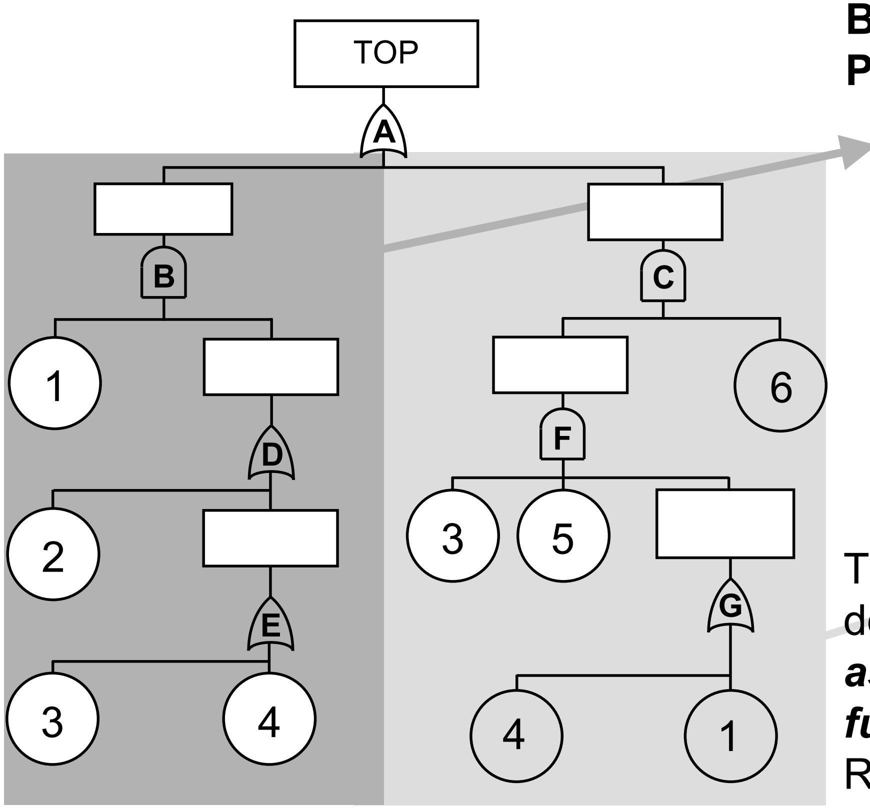
These Minimal Cut Sets…

1	2		
1	3		
1	4		
3	4	5	6

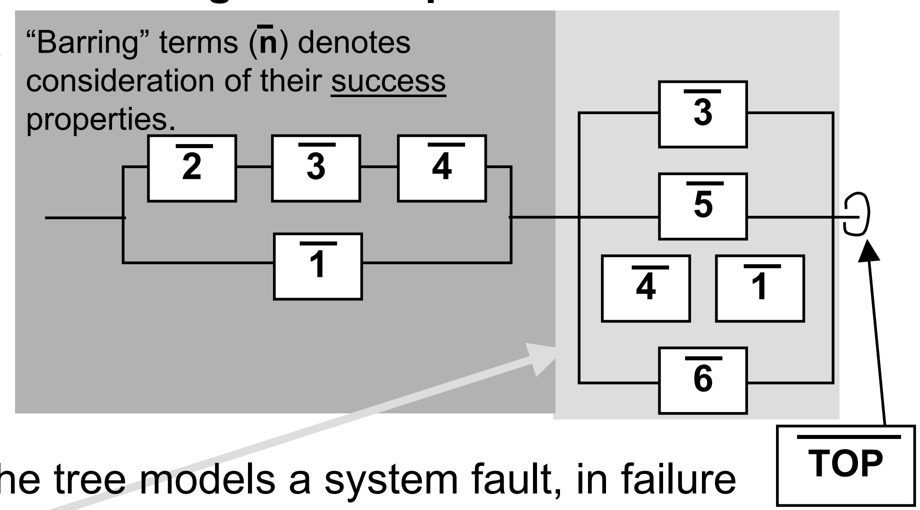
represent this Fault Tree – a Logic Equivalent of the original tree.



From Tree to Reliability Block Diagram



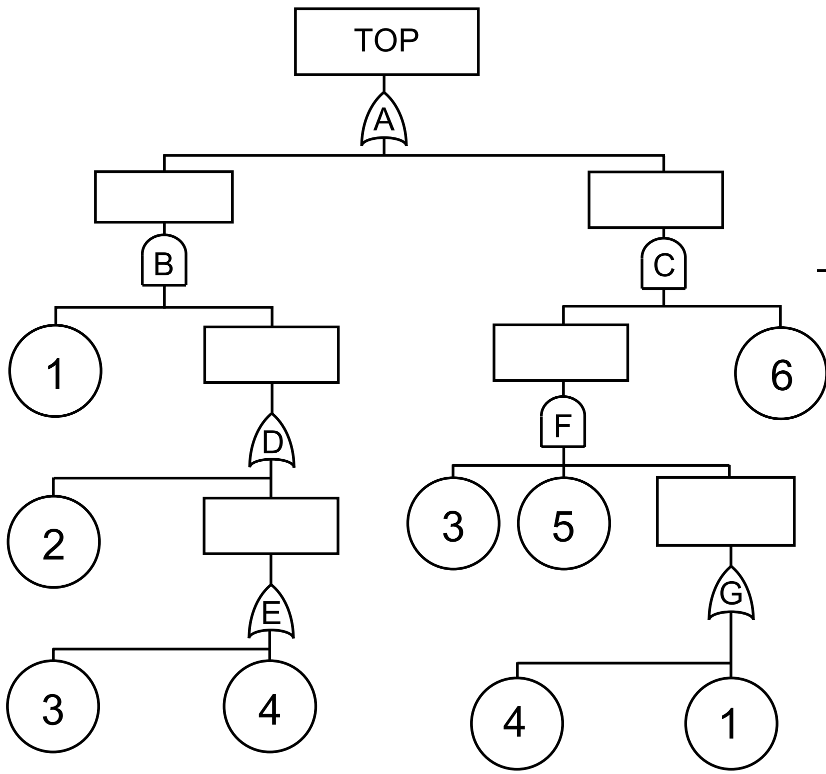
Blocks represent functions of system elements. Paths through them represent success.

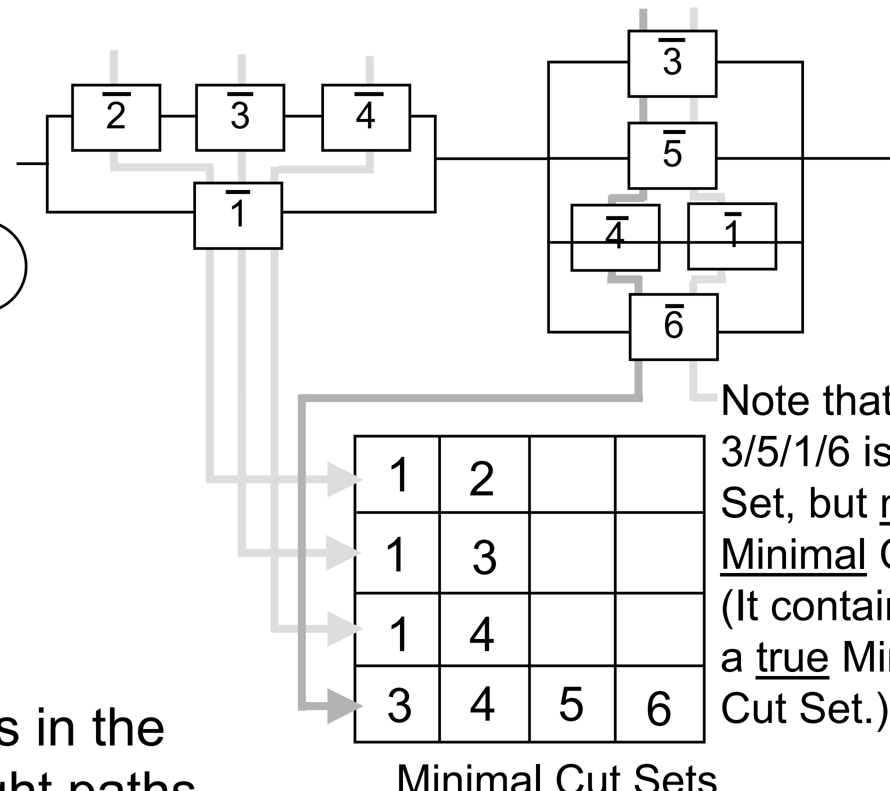


The tree models a system fault, in failure domain. Let that fault be ***System Fails to Function as Intended***. Its opposite, ***System Succeeds to function as intended***, can be represented by a Reliability Block Diagram in which success flows through system element functions from left to right. Any path through the block diagram, not interrupted by a fault of an element, results in system success.

JACOBS SVERDRUP

Cut Sets and Reliability Blocks





Note that 3/5/1/6 is a Cut Set, but not a Minimal Cut Set. (It contains 1/3, a true Minimal Cut Set.)

Each Cut Set (horizontal rows in the matrix) interrupts all left-to-right paths through the Reliability Block Diagram

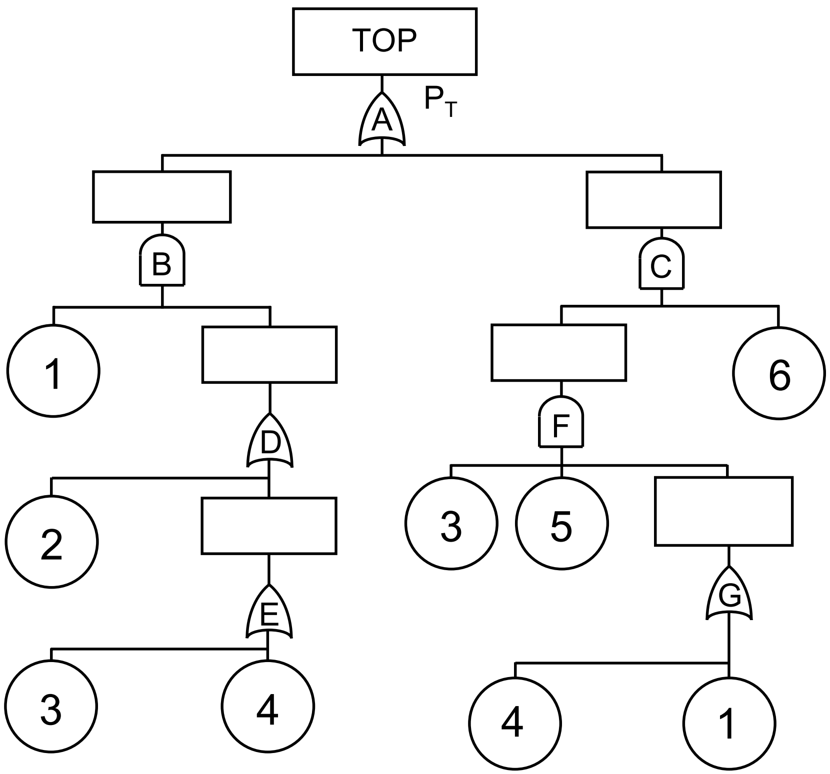
JACOBS SVERDRUP

Cut Set Uses

- Evaluating P_T
- Finding Vulnerability to Common Causes
- Analyzing Common Cause Probability
- Evaluating Structural Cut Set "Importance"
- Evaluating Quantitative Cut Set "Importance"
- Evaluating Item "Importance"

JACOBS SVERDRUP

Cut Set Uses/Evaluating P_T



Cut Set Probability (P_k), the product of probabilities for events within the Cut Set, is the probability that the Cut Set being considered will induce TOP.

$$P_k = \Pi P_e = P_1 \times P_2 \times P_3 \times \ldots P_n$$

Minimal Cut Sets

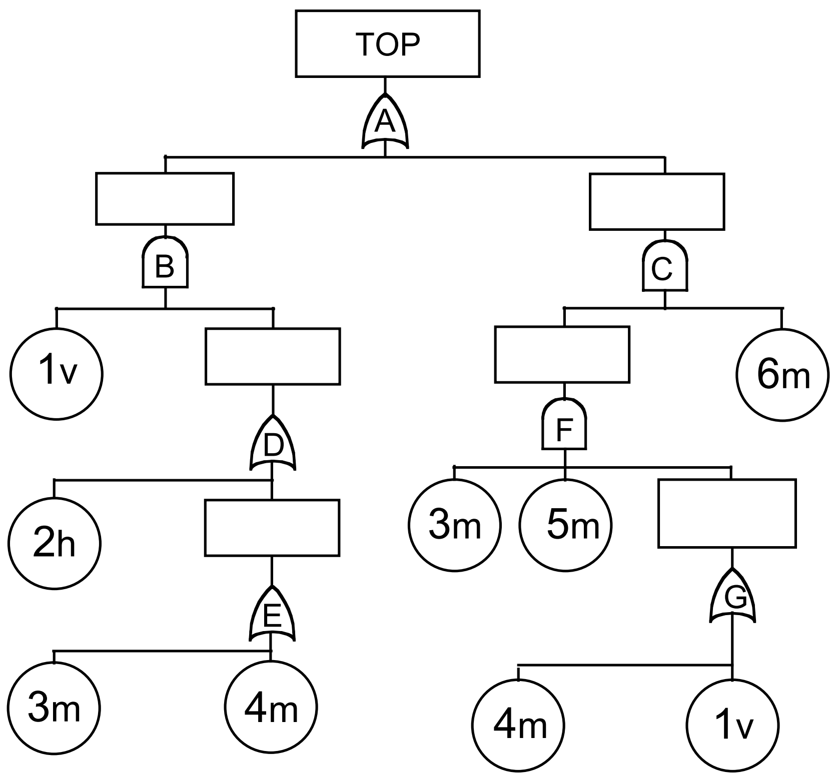
1	2		
1	3		
1	4		
3	4	5	6

$$P_t \cong \Sigma P_k =$$
$$P_1 \times P_2 +$$
$$P_1 \times P_3 +$$
$$P_1 \times P_4 +$$
$$P_3 \times P_4 \times P_5 \times P_6$$

Note that propagating probabilities through an “unpruned” tree, i .e., using Boolean-Indicated Cut Sets rather than minimal Cut Sets, would produce a falsely high P_T.

1	2		
3	5	4	6
1	3		
1	4		
3	5	1	6

Cut Set Uses/Common Cause Vulnerability



Uniquely subscript initiators, using letter indicators of common cause susceptibility, e.g….

ℓ = location (code *where*)
m = moisture
h = human operator
q = heat
f = cold
v = vibration
…etc.

Minimal Cut Sets

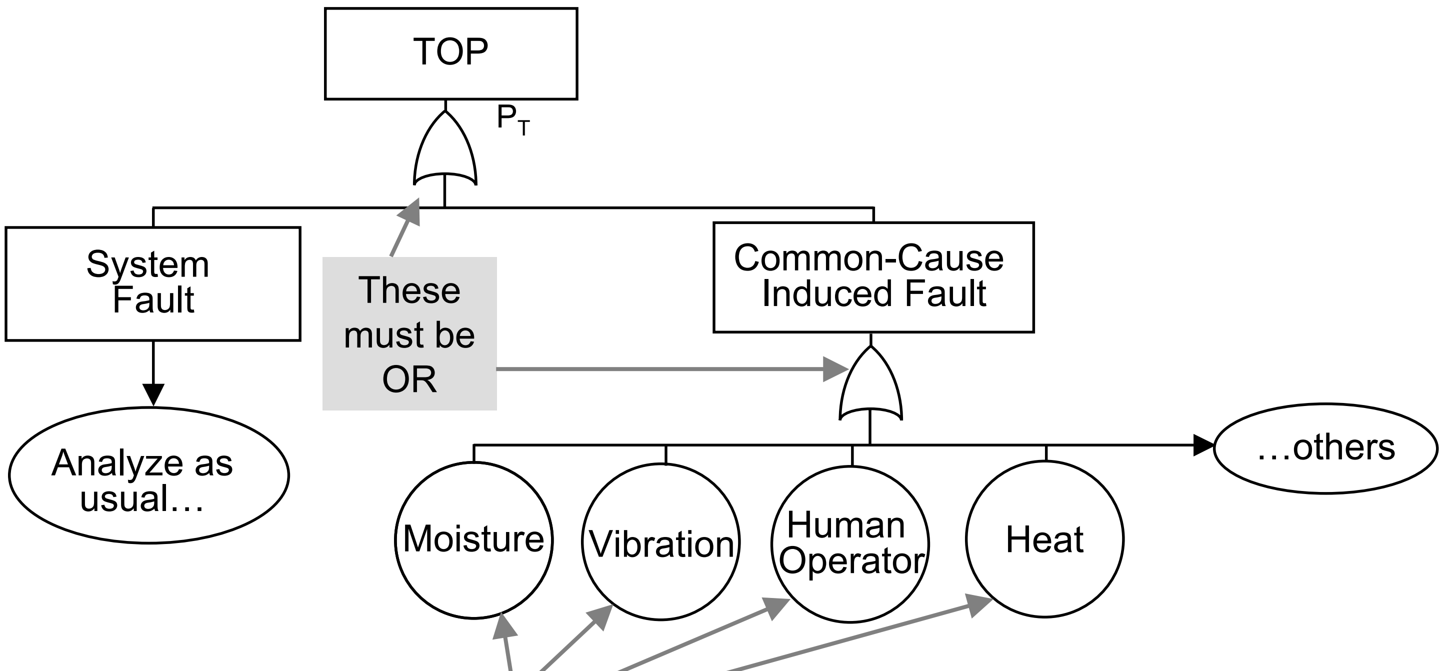
1v	2h		
1v	3m		
1v	4m		
3m	4m	5m	6m

All Initiators in this Cut Set are vulnerable to moisture. Moisture is a Common Cause and can induce TOP. **ADVICE**: Moisture proof one or more items.

Some Initiators may be vulnerable to several Common Causes and receive several corresponding subscript designators. Some may have no Common Cause vulnerability – receive no subscripts.

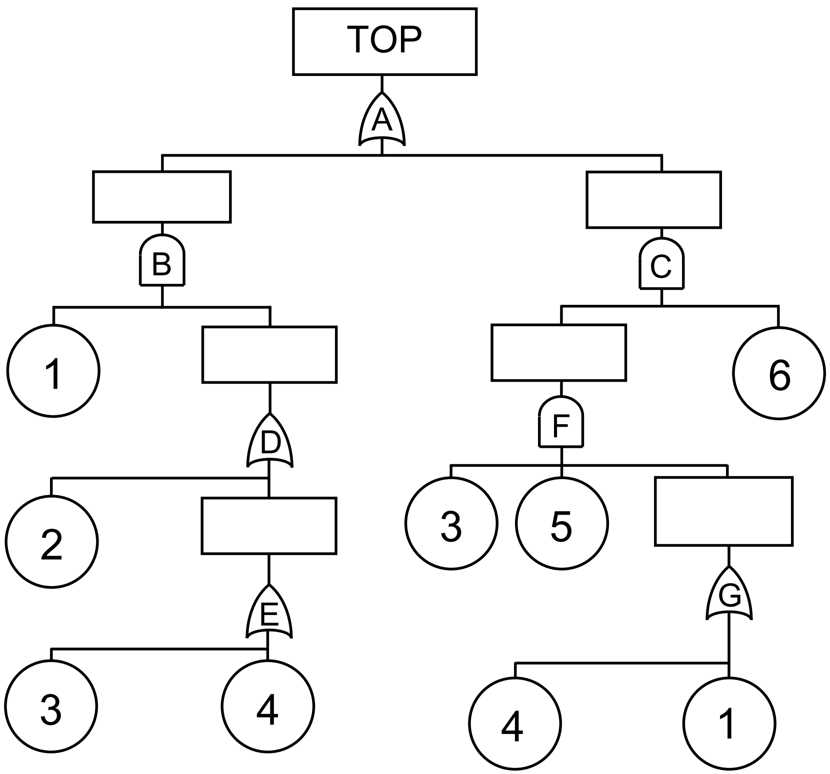
JACOBS SVERDRUP

Analyzing Common Cause Probability



Introduce each Common Cause identified as a “Cut Set Killer” at its individual probability level of both (1) occurring, and (2) inducing all terms within the affected cut set.

Cut Set Structural "Importance"



Minimal Cut Sets

1	2		
1	3		
1	4		
3	4	5	6

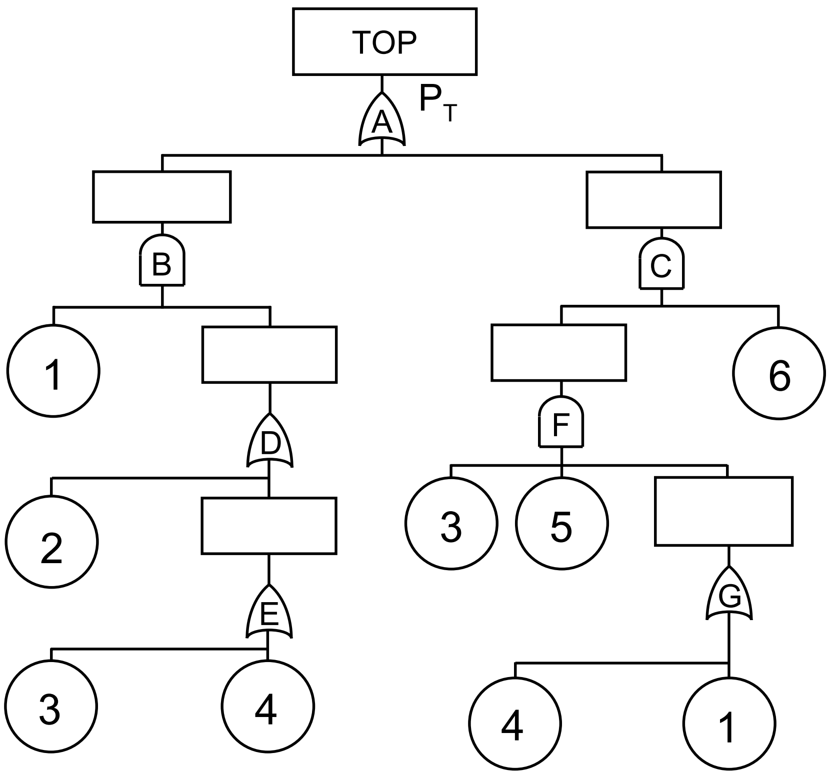
All other things being equal…
- A **LONG Cut Set** signals low vulnerability
- A **SHORT Cut Set** signals higher vulnerability
- Presence of **NUMEROUS Cut Sets** signals high vulnerability

...and a singlet cut set signals a Potential **Single-Point Failure**.

Analyzing Structural Importance enables qualitative ranking of contributions to System Failure.

JACOBS SVERDRUP

Cut Set Quantitative "Importance"



The quantitative importance of a Cut Set (I_k) is the numerical probability that, given that TOP has occurred, that Cut Set has induced it.

$$I_k = \frac{P_k}{P_T}$$

…where $P_k = \Pi \, P_e = P_3 \times P_4 \times P_5 \times P_6$

Minimal Cut Sets

1	2		
1	3		
1	4		
3	4	5	6

Analyzing Quantitative Importance enables numerical ranking of contributions to System Failure. To reduce system vulnerability most effectively, attack Cut Sets having greater Importance. Generally, short Cut Sets have greater Importance, long Cut Sets have lesser Importance.

Item 'Importance"

The quantitative Importance of an item (I_e) is the numerical probability that, given that TOP has occurred, that item has contributed to it.

$$I_e \cong \sum^{N_e} I_{ke}$$

N_e = Number of Minimal Cut Sets containing Item *e*

I_{ke} = Importance of the Minimal Cuts Sets containing Item *e*

Minimal Cut Sets

1	2		
1	3		
1	4		
3	4	5	6

Example – Importance of item 1…

$$I_1 \cong \frac{(P_1 \text{ x } P_2) + (P_1 \text{ x } P_3) + (P_1 \text{ x } P_4)}{P_T}$$

Path Sets

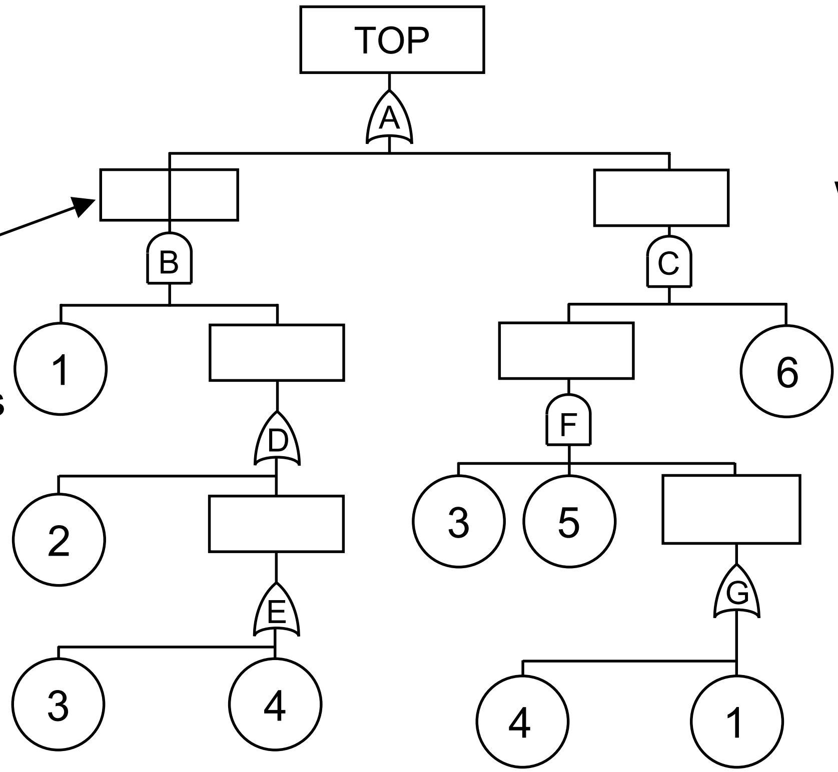
Aids to…

- Further Diagnostic Measures
- Linking to Success Domain
- Trade/Cost Studies

- A **PATH SET** is a group of fault tree initiators which, if none of them occurs, will guarantee that the **TOP** event cannot occur.
- **TO FIND PATH SETS*** change all **AND** gates to **OR** gates and all **OR** gates to **AND**. Then proceed using matrix construction as for Cut Sets. Path Sets will be the result.

*This Cut Set-to-Path-Set conversion takes advantage of de Morgan's duality theorem. Path Sets are <u>complements</u> of Cut Sets.

A Path Set Example



Path Sets are least groups of initiators which, if they <u>cannot</u> occur, <u>guarantee against</u> TOP occurring

This Fault Tree has these Minimal Cut sets

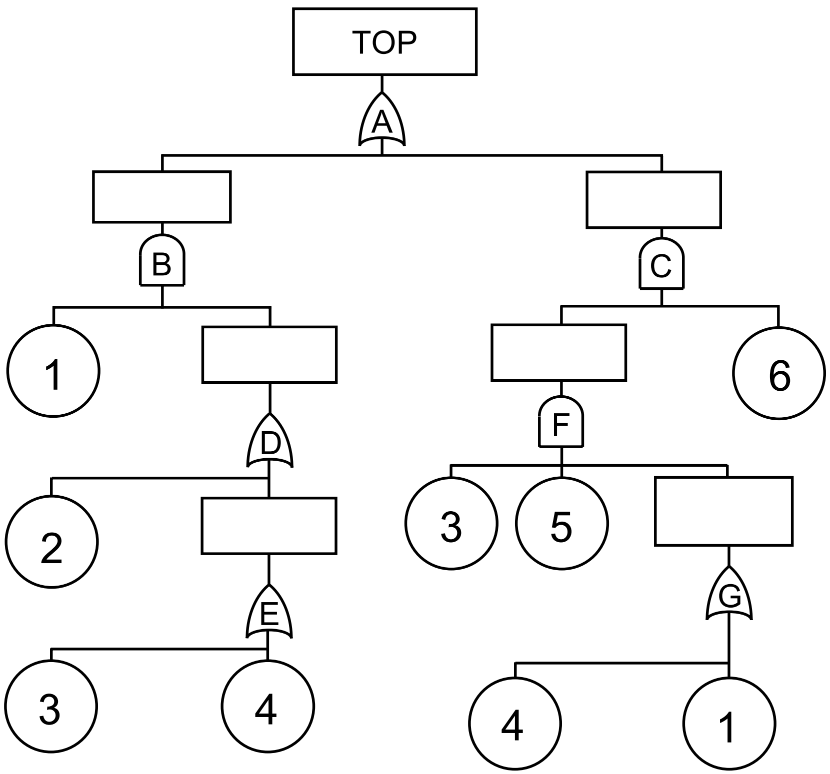
1	2		
1	3		
1	4		
3	4	5	6

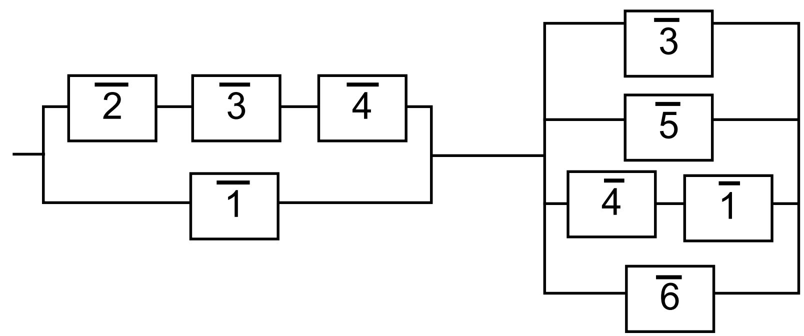
…and these Path Sets

$\overline{1}$	$\overline{3}$	
$\overline{1}$	$\overline{4}$	
$\overline{1}$	$\overline{5}$	
$\overline{1}$	$\overline{6}$	
$\overline{2}$	$\overline{3}$	$\overline{4}$

"Barring" terms ($\overline{\mathbf{n}}$) denotes consideration of their <u>success</u> properties

Path Sets and Reliability Blocks



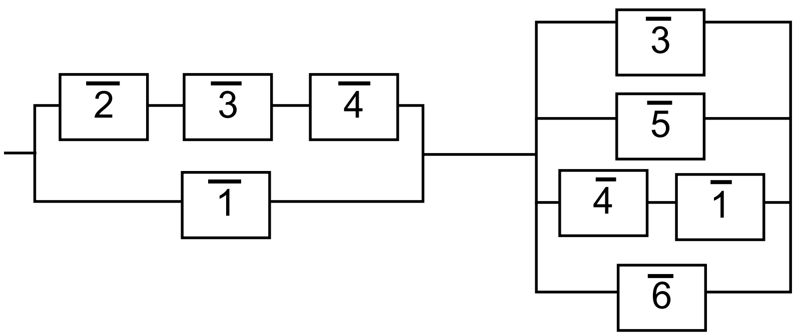


$\overline{1}$	$\overline{3}$	
$\overline{1}$	$\overline{4}$	
$\overline{1}$	$\overline{5}$	
$\overline{1}$	$\overline{6}$	
$\overline{2}$	$\overline{3}$	$\overline{4}$

Path Sets

Each Path Set (horizontal rows in the matrix) represents a left-to-right path through the Reliability Block Diagram.

Pat Sets and Trade Studies



$$P_p \cong \Sigma P_e$$

Path Set Probability (P_p) is the probability that the system will suffer a fault at one or more points along the operational route modeled by the path. To minimize failure probability, minimize path set probability.

	Path Sets			ΔP_p	$\Delta \$$
a	$\overline{1}$	$\overline{3}$		ΔP_{Pa}	$\Delta \$_a$
b	$\overline{1}$	$\overline{4}$		ΔP_{Pb}	$\Delta \$_b$
c	$\overline{1}$	$\overline{5}$		ΔP_{Pc}	$\Delta \$_c$
d	$\overline{1}$	$\overline{6}$		ΔP_{Pd}	$\Delta \$_d$
e	$\overline{2}$	$\overline{3}$	$\overline{4}$	ΔP_{Pe}	$\Delta \$_e$

Sprinkle countermeasure resources amongst the Path Sets. Compute the probability decrement for each newly adjusted Path Set option. Pick the countermeasure ensemble(s) giving the most favorable $\Delta P_p / \Delta \$$. (Selection results can be verified by computing $\Delta P_T / \Delta \$$ for competing candidates.)

JACOBS SVERDRUP

Reducing Vulnerability – A Summary

- Inspect tree – find/operate on major P_T contributors…
  - Add interveners/redundancy (lengthen cut sets).
  - Derate components (increase robustness/reduce P_e).
  - Fortify maintenance/parts replacement (increase MTBF).
- Examine/alter system architecture – increase path set/cut set ratio.
- Evaluate Cut Set Importance. Rank items using I_k.} $I_k = P_k / P_T$
  Identify items amenable to improvement.
- Evaluate item importance. Rank items using I_e.} $I_e \cong \sum^{N_e} I_{ke}$
  Identify items amenable to improvement.
- Evaluate path set probability.
  Reduce P_P at most favorable $\Delta P / \Delta \$$. } $P_p \cong \sum P_e$

For <u>all</u> new countermeasures, THINK… • **COST** • **EFFECTIVENESS** • **FEASIBILITY** (incl. schedule)

AND

Does the new countermeasure… • Introduce new **HAZARDS**? • Cripple the system?

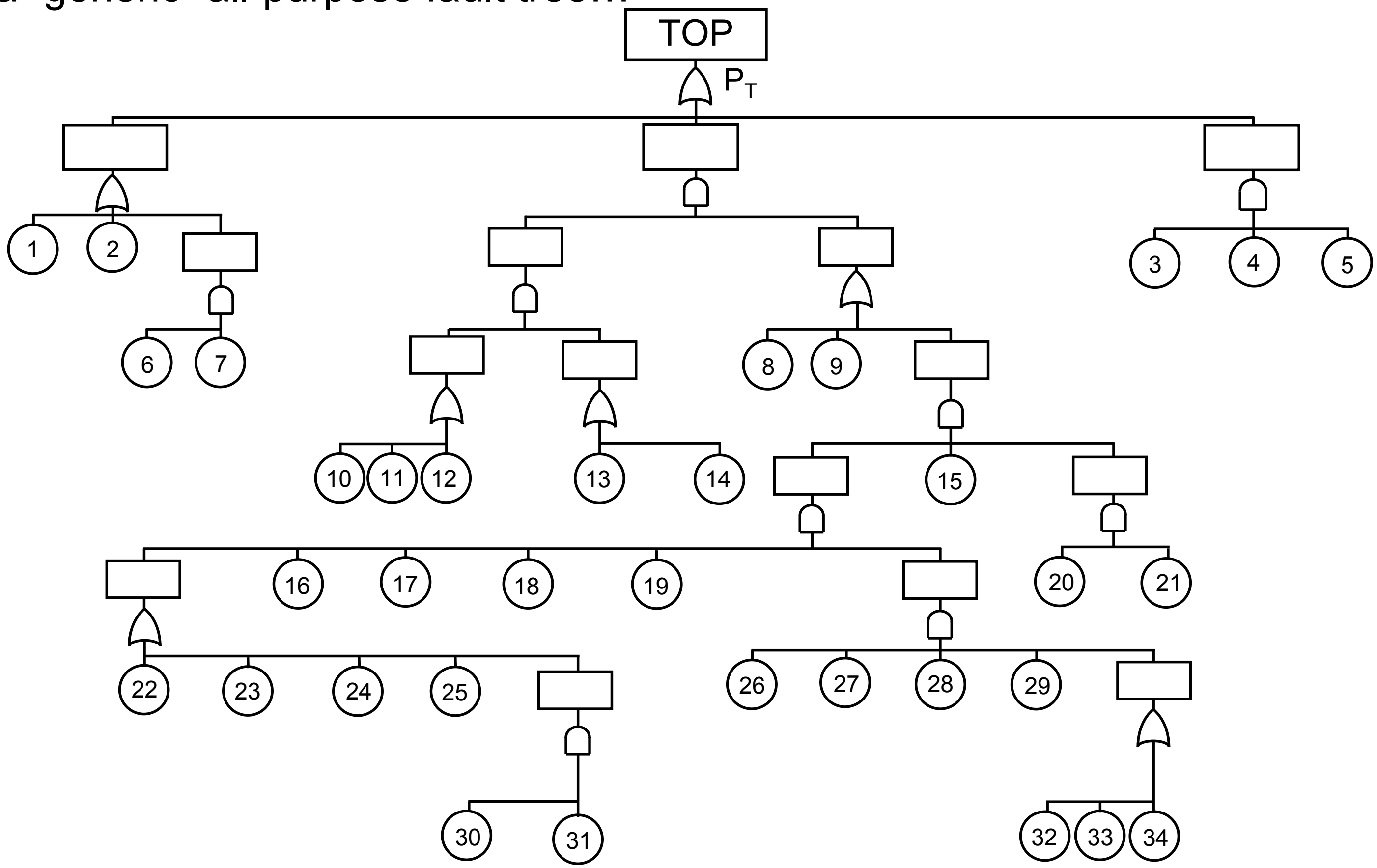
JACOBS SVERDRUP

Some Diagnostic and Analytical Gimmicks

- A Conceptual Probabilistic Model
- Sensitivity Testing
- Finding a P_T Upper Limit
- Limit of Resolution – Shutting off Tree Growth
- State-of-Component Method
- When to Use Another Technique – FMECA

Some Diagnostic Gimmicks

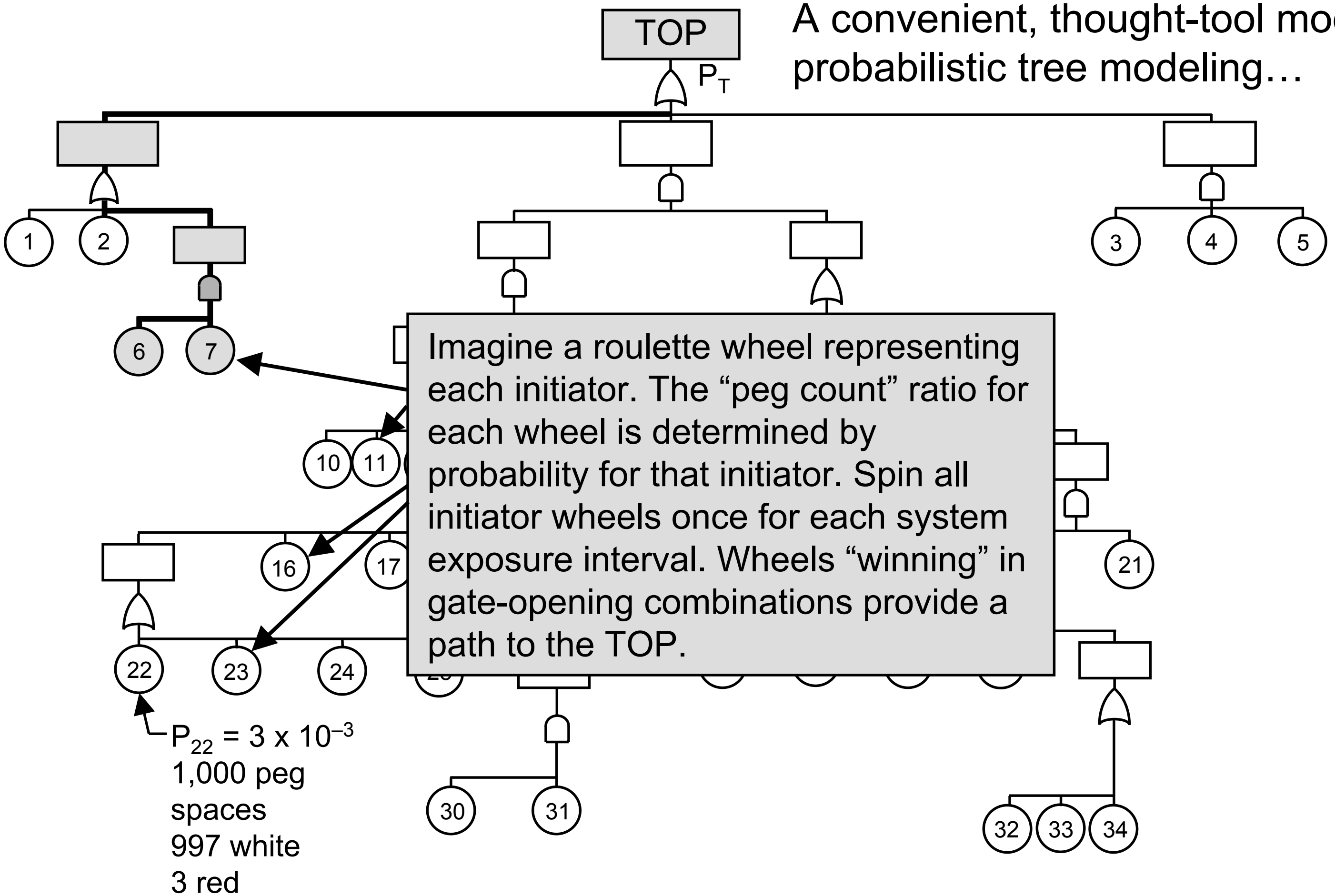
Using a “generic” all-purpose fault tree…



JACOBS SVERDRUP

Think "Roulette Wheels"

A convenient, thought-tool model of probabilistic tree modeling…

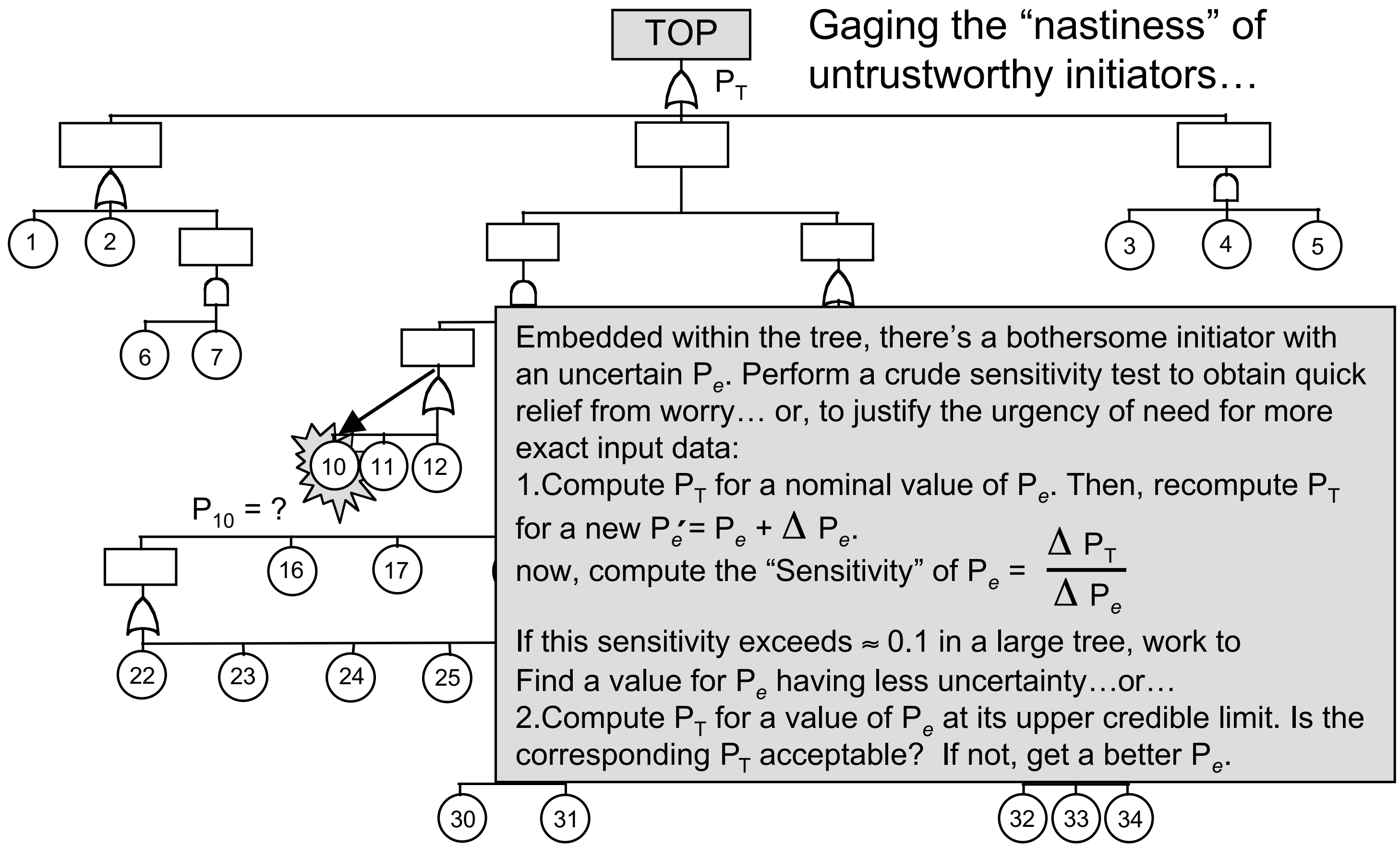


Imagine a roulette wheel representing each initiator. The "peg count" ratio for each wheel is determined by probability for that initiator. Spin all initiator wheels once for each system exposure interval. Wheels "winning" in gate-opening combinations provide a path to the TOP.

JACOBS SVERDRUP

Use Sensitivity Tests

Gaging the “nastiness” of untrustworthy initiators…



Embedded within the tree, there’s a bothersome initiator with an uncertain P_e. Perform a crude sensitivity test to obtain quick relief from worry… or, to justify the urgency of need for more exact input data:

1. Compute P_T for a nominal value of P_e. Then, recompute P_T for a new $P_e' = P_e + \Delta P_e$.

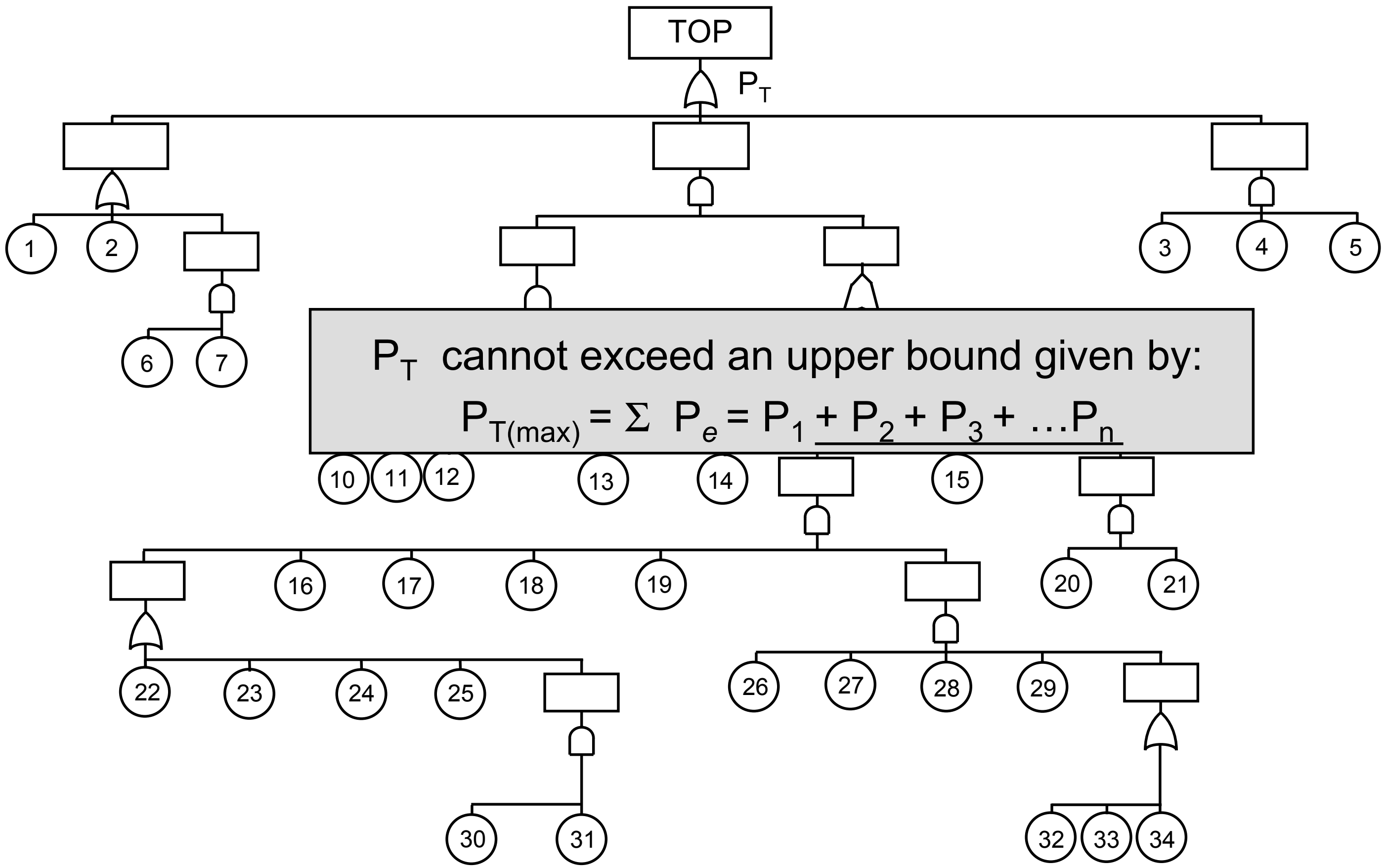
   now, compute the “Sensitivity” of $P_e = \dfrac{\Delta P_T}{\Delta P_e}$

   If this sensitivity exceeds ≈ 0.1 in a large tree, work to Find a value for P_e having less uncertainty…or…

2. Compute P_T for a value of P_e at its upper credible limit. Is the corresponding P_T acceptable? If not, get a better P_e.

Find a Max P_T Limit Quickly

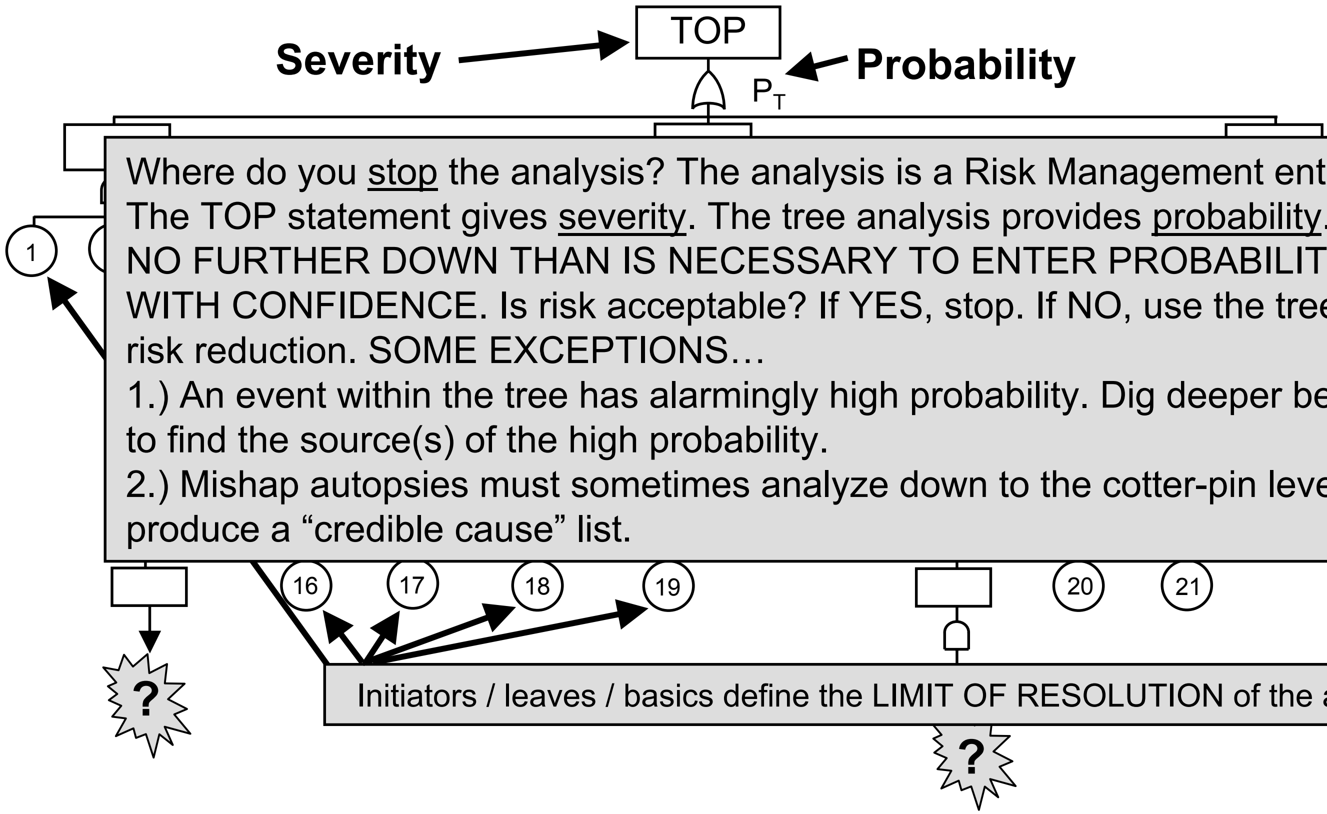
The "parts-count" approach gives a sometimes-useful early estimate of P_T…



P_T cannot exceed an upper bound given by:

$$P_{T(max)} = \Sigma \; P_e = P_1 + P_2 + P_3 + \ldots P_n$$

How Far Down Should a Fault Tree Grow?



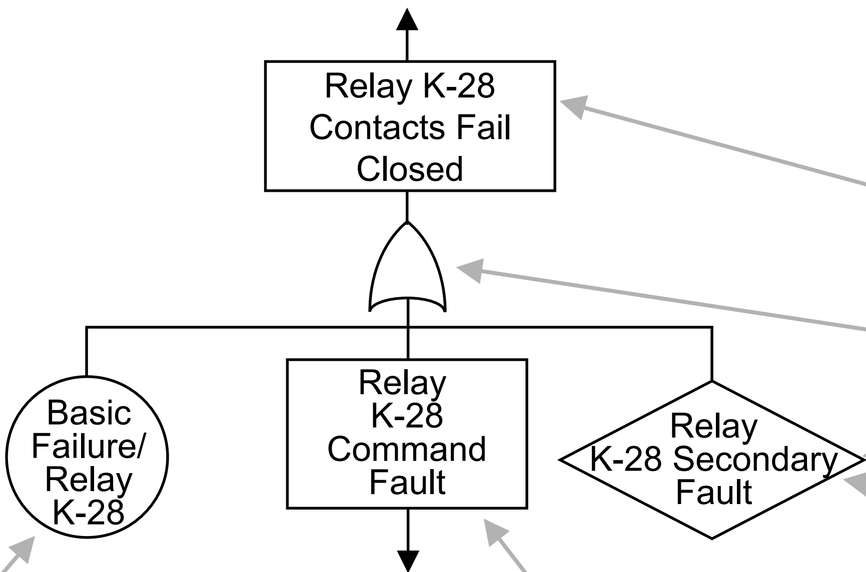
Where do you stop the analysis? The analysis is a Risk Management enterprise. The TOP statement gives severity. The tree analysis provides probability. ANALYZE NO FURTHER DOWN THAN IS NECESSARY TO ENTER PROBABILITY DATA WITH CONFIDENCE. Is risk acceptable? If YES, stop. If NO, use the tree to guide risk reduction. SOME EXCEPTIONS…

1.) An event within the tree has alarmingly high probability. Dig deeper beneath it to find the source(s) of the high probability.

2.) Mishap autopsies must sometimes analyze down to the cotter-pin level to produce a “credible cause” list.

Initiators / leaves / basics define the LIMIT OF RESOLUTION of the analysis.

State-of-Component Method



WHEN – Analysis has proceeded to the device level – i.e., valves, pumps, switches, relays, etc.

HOW – Show device fault/failure in the mode needed for upward propagation.

Install an OR gate.

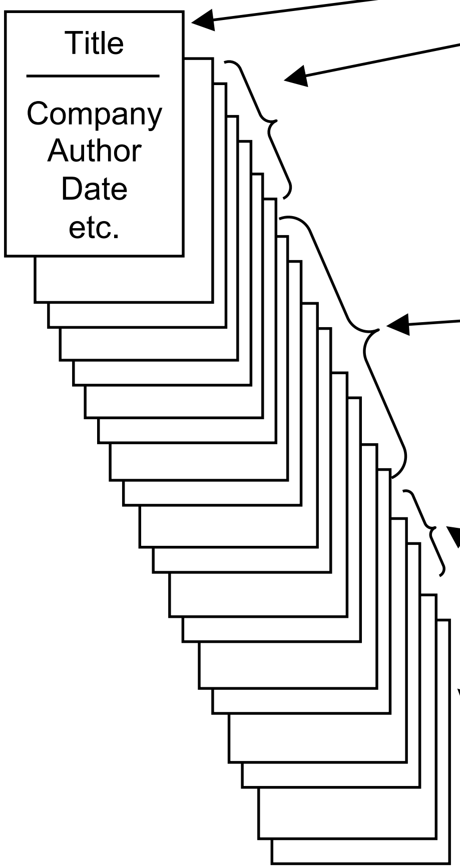
Place these three events beneath the OR.

This represents internal "self" failures under normal environmental and service stresses – e.g., coil burnout, spring failure, contacts drop off…

Analyze further to find the *source* of the fault condition, induced by presence/absence of external command "signals." (Omit for most passive devices – e.g., piping.)

This represents faults from environmental and service stresses for which the device is not qualified – e.g., component struck by foreign object, wrong component selection/installation. (Omit, if negligible.)

The Fault Tree Analysis Report



Executive Summary (Abstract of complete report)

Scope of the analysis…

Brief system description

TOP Description/Severity Bounding

Analysis Boundaries

- Physical Boundaries
- Operational Boundaries
- Operational Phases
- Human Operator In/out
- Interfaces Treated
- Resolution Limit
- Exposure Interval
- Others…

Say what <u>is</u> analyzed and what is <u>not</u> analyzed.

The Analysis

Discussion of Method (Cite Refs.)

Software Used

Presentation/Discussion of the Tree

Source(s) of Probability Data (If quantified)

Common Cause Search (If done)

Sensitivity Test(s) (If conducted)

Cut Sets (Structural and/or Quantitative Importance, if analyzed)

Path Sets (If analyzed)

Trade Studies (If Done)

Show Tree as Figure. Include Data Sources, Cut Sets, Path Sets, etc. as Tables.

Findings…

TOP Probability (Give Confidence Limits)

Comments on System Vulnerability

Chief Contributors

Candidate Reduction Approaches (If appropriate)

Conclusions and Recommendations…

Risk Comparisons (“Bootstrapping” data, if appropriate)

Is further analysis needed? By what method(s)?

JACOBS SVERDRUP

FTA vs. FMECA Selection Criteria*

Selection Characteristic	Preferred	
	FTA	FMECA
Safety of public/operating/maintenance personnel	√	
Small number/clearly defined TOP events	√	
Indistinctly defined TOP events		√
Full-Mission completion critically important	√	
Many, potentially successful missions possible		√
"All possible" failure modes are of concern		√
High potential for "human error" contributions	√	
High potential for "software error" contributions	√	
Numerical "risk evaluation" needed	√	
Very complex system architecture/many functional parts	√	
Linear system architecture with little/human software influence		√
System irreparable after mission starts	√	

*Adapted from "Fault Tree Analysis Application Guide," Reliability Analysis Center, Rome Air Development Center.

JACOBS SVERDRUP

Fault Tree Constraints and Shortcomings

- Undesirable events must be foreseen and are only analyzed singly.
- All significant contributors to fault/failure must be anticipated.
- Each fault/failure initiator must be constrained to two conditional modes when modeled in the tree.
- Initiators at a given analysis level beneath a common gate must be independent of each other.
- Events/conditions at any analysis level must be true, immediate contributors to next-level events/conditions.
- Each Initiator's failure rate must be a predictable constant.

JACOBS SVERDRUP

Common Fault Tree Abuses

- Over-analysis – “Fault Kudzu”
- Unjustified confidence in numerical results – 6.0232×10^{-5}…+/–?
- Credence in preposterously low probabilities – 1.666×10^{-24}/hour
- Unpreparedness to deal with results (particularly quantitative) – Is 4.3×10^{-7}/hour acceptable for a catastrophe?
- Overlooking common causes – Will a roof leak or a shaking floor wipe you out?
- Misapplication – Would Event Tree Analysis (or another technique) serve better?
- Scoping changes in mid-tree

Fault Tree Payoffs

- Gaging/quantifying system failure probability.
- Assessing system Common Cause vulnerability.
- Optimizing resource deployment to control vulnerability.
- Guiding system reconfiguration to reduce vulnerability.
- Identifying Man Paths to disaster.
- Identifying potential single point failures.
- Supporting trade studies with differential analyses.

FAULT TREE ANALYSIS is a risk assessment enterprise. Risk Severity is defined by the TOP event. Risk Probability is the result of the tree analysis.

JACOBS SVERDRUP

Closing Caveats

- Be wary of the **ILLUSION** of **SAFETY**. Low probability does not mean that a mishap won't happen!
- **THERE IS NO ABSOLUTE SAFETY**! An enterprise is safe only to the degree that its risks are tolerable!
- Apply broad confidence limits to probabilities representing human performance!
- A large number of systems having low probabilities of failure means that **A MISHAP WILL HAPPEN** – *somewhere* among them!

$$P_1 + P_2 + P_3 + P_4 + \text{----------} P_n \approx 1$$

More…

JACOBS SVERDRUP

Do you REALLY have enough data to justify QUANTITATIVE ANALYSIS?

For 95% confidence…

We must have no failures in		to give $P_F \cong$…	and $\Re \cong$ …
Assumptions: ■ Stochastic System Behavior ■ Constant System Properties ■ Constant Service Stresses ■ Constant Environmental Stresses	1,000 tests	3×10^{-3}	0.997
	300 tests	10^{-2}	0.99
	100 tests	3×10^{-2}	0.97
	30 tests	10^{-1}	0.9
	10 tests	3×10^{-1}	0.7

Don't drive the numbers into the ground!

JACOBS SVERDRUP

Analyze Only to Turn Results Into Decisions

"Perform an analysis only to reach a decision. Do not perform an analysis if that decision can be reached without it. It is not effective to do so. It is a waste of resources."

Dr. V.L. Grose

George Washington University

JACOBS SVERDRUP