SAND2014-17534C

Fault Tree Analysis (Overview for ASSE)

Experimental Operations
Sandia National Laboratories
9/2014

Ron Pedersen, DMTS

Thanks to Kevin J. Maloney

July 9, 2011

References:

NST416

NUREG0492

Relex

NASA Fault Tree Handbook

OUTLINE

- Origin of Fault Tree Analysis
- Uses for Fault Trees
- Fault Tree Terminology
  - Faults and Failures
  - Symbols
  - Structure
  - Results
- FTA example
  - Structure
  - Boolean Algebra
  - Results
    - Cut sets
    - Importance levels
- Thermal Test Simple Example
- FTA Results

HISTORY OF FTA

- Developed by H. Watson and Allison Mearns of Bell Labs for use on the Minute Man Guidance System in 1962
- Boeing expanded its use to the MMII and their own civilian aircraft by 1966
  - D.F. Hassl
- Codified for use by the FAA in 10CFR25.1309 by 1970
- NRC Fault Tree Handbook, NUREG-0492, in 1975.
  - Expanded use for PRA after TMI in 1979
- Sandia: Set Equation Transformation System (SETS), 1977
- OSHA codified it use in 19CFR1910.119 after Bhopal and Piper Alpha accidents (1984-1992) for Process Hazard Analysis
- Accepted for use in several international industrial and military standards
  - MIL-HDBK-338
  - NASA
  - International Electrotechnical Commission

SNL Uses for Fault Trees

Weapon Systems

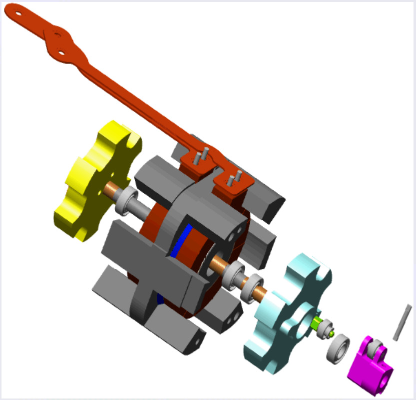
•Weapon Development Phases

•Safety-critical feature identification and configuration management

• Nuclear Weapon Safety Assurance and Assessment

Testers

Weapon Components



Nuclear Reactor Safety

Other:

- *Human Factors*
- *Reliability*
- *WP&C ES*

Fault Tree Analysis - Definition

- Fault tree analysis is…
  - A deductive *analytical* technique…
  - whereby an *undesired state* of a system is specified…
  - the system is then analyzed in the context of its *environment and operation*…
  - to find all *credible ways* in which the undesired system state can occur

A Top-down approach

NUREG -0492

Why Build a Fault Tree?

Qualitative (Most important for us)

- Identify combinations of system failures
  - Find ‘First-Order’ Faults
  - “Single-Point Failures” (WP&C Criteria for Safe Design and Operations, MN471021)
- Identify critical components, procedures, and tasks
- Design aid
- Understanding what you are depending on for safety in your system – engineered controls, administrative controls, PPE, etc.

Quantitative (Active Safety or for Reliability analysis)

- System unavailability
- Frequency/probability of undesired event

Faults versus Failures

Fault

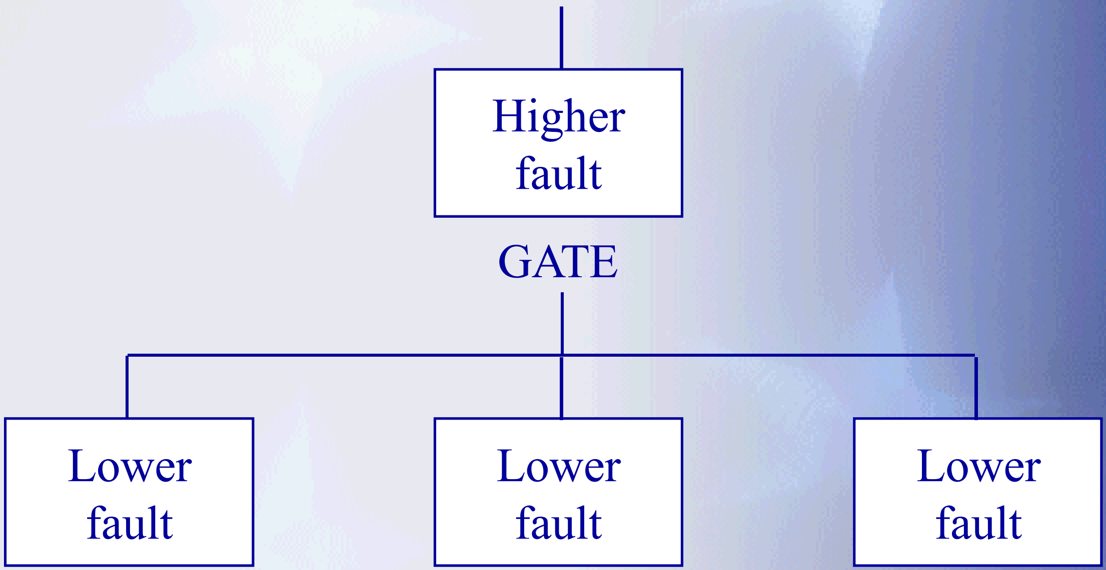
- The occurrence or existence of an undesired state for a component, subsystem, or system
  - Example: Solenoid propane valve temporarily freezes open or closed
- Sneak circuits (electrical, pneumatic, hydraulic) are faults – nothing failed, just an unintended, unexpected, response.

Failure

- Basic abnormal event that renders a component, subsystem, or system incapable of performing its intended function
- Represented by primary events on a fault tree
  - Example: Hose breaks

All failures are faults, but not all faults are failures

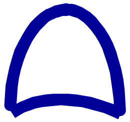
Fault Tree Gate Function

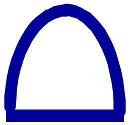


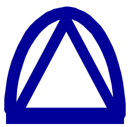
- Fault tree is constructed by proceeding from the higher (general) to the lower faults (specific)
- Inputs (lower faults) relate to the outputs (higher faults) through gates

FAULT TREE EVENT SYMBOLS

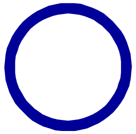
Gate Symbols

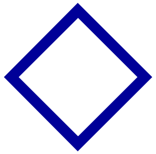

OR gate


AND gate


Priority AND gate

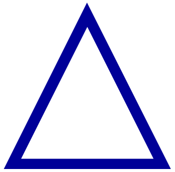
Primary Event Symbols


Basic event


Undeveloped event

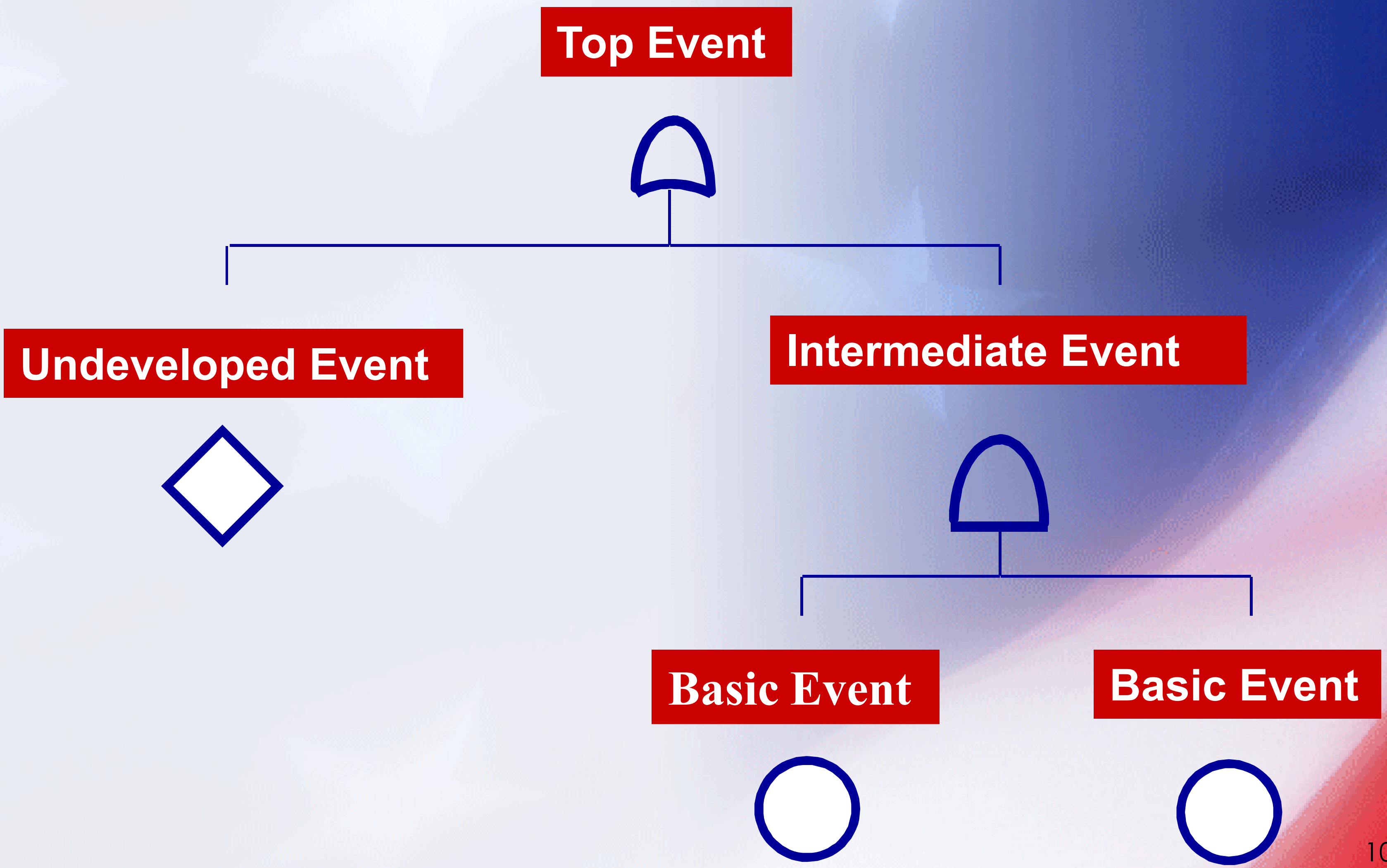
Other Symbols


Remarks


Transfer

Advanced Features:
NAND, NOR, XOR, NOT, Voting gates, Inhibit gates, Sequence Enforcing gates

FAULT TREE STRUCTURE



Fault Tree Construction - General

Completeness (and value) in fault tree construction is achieved by:

- Thorough understanding of the system
- Thoughtful definition of top event
- Careful definition of each fault
- Taking small steps in logic
- Being exhaustive at each step

Avoid:
“That could never happen”
“We never had a failure/fault before”

Failure Space vs. Success Space
Red Thinking vs. Blue Thinking

Top Event Definition

Process begins by defining the Top Event in the fault tree diagram and working down from there . After the fault tree top event is defined:

Unacceptable Consequences

- Analyst determines the immediate, necessary and sufficient causes for the top event occurrence
- Continue identifying the immediate, necessary and sufficient causes until all faults have been resolved into their elementary faults or failures
- Usually quit at a level of detail where features are identifiable, controllable, or easily measurable
  - Hydraulic coupler vs. coupler metallic composition
  - Pressure regulator vs. internal parts

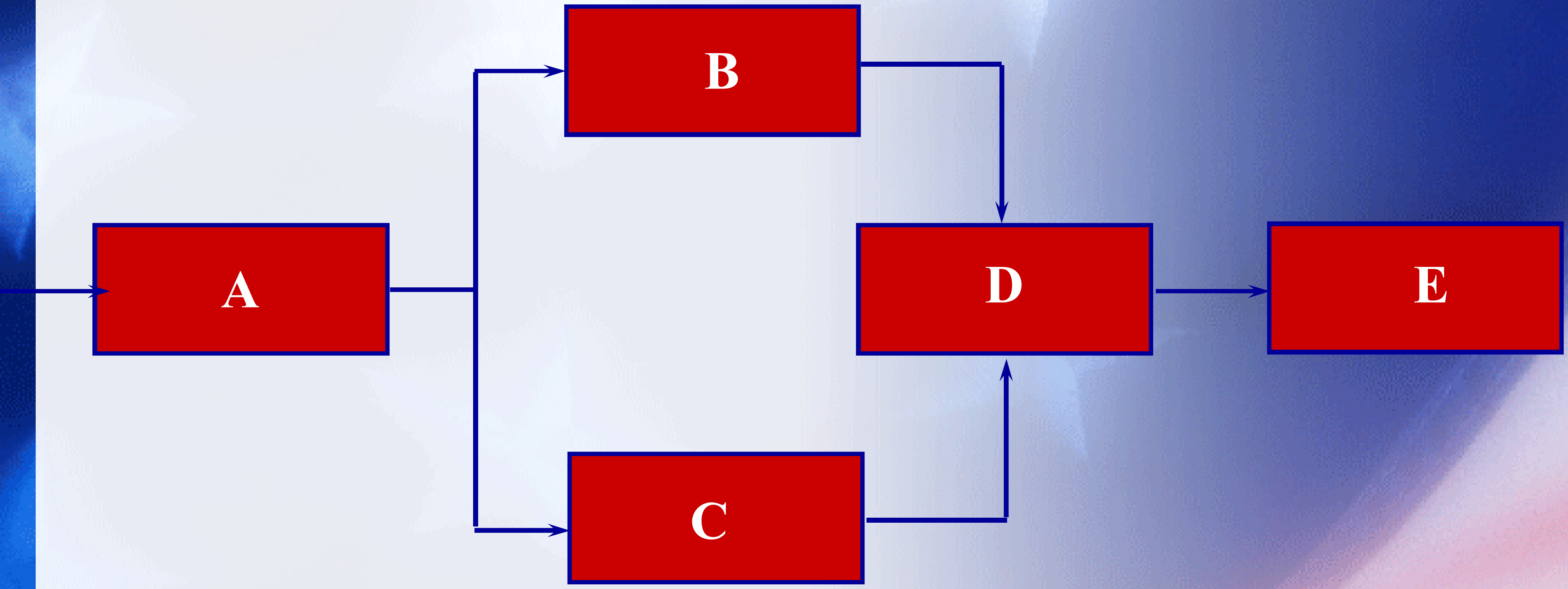
Controls

Fault Tree Evaluation - Cut Sets

- Solution of the fault tree provides the *"cut set expression"*
  - <u>Cut set</u> - any combination of basic events that is sufficient to cause the top event to occur
  - <u>Minimal cut set</u> - any combination of primary events that is necessary and sufficient to cause the top event to occur
    - Redundancy has been eliminated
  - <u>First-order fault</u> (Single Point Failure) – a minimal cut set containing only one event.
    - This single basic event is sufficient to cause system failure
    - "OR GATE" rule of thumb

Note:
Second-order cut sets containing only administrative controls may be of greater concern than having an engineered control first-order fault
Note:
A Basic Event reoccurring in several Multi-order cut sets indicates importance of that Basic Event

Example System Diagram



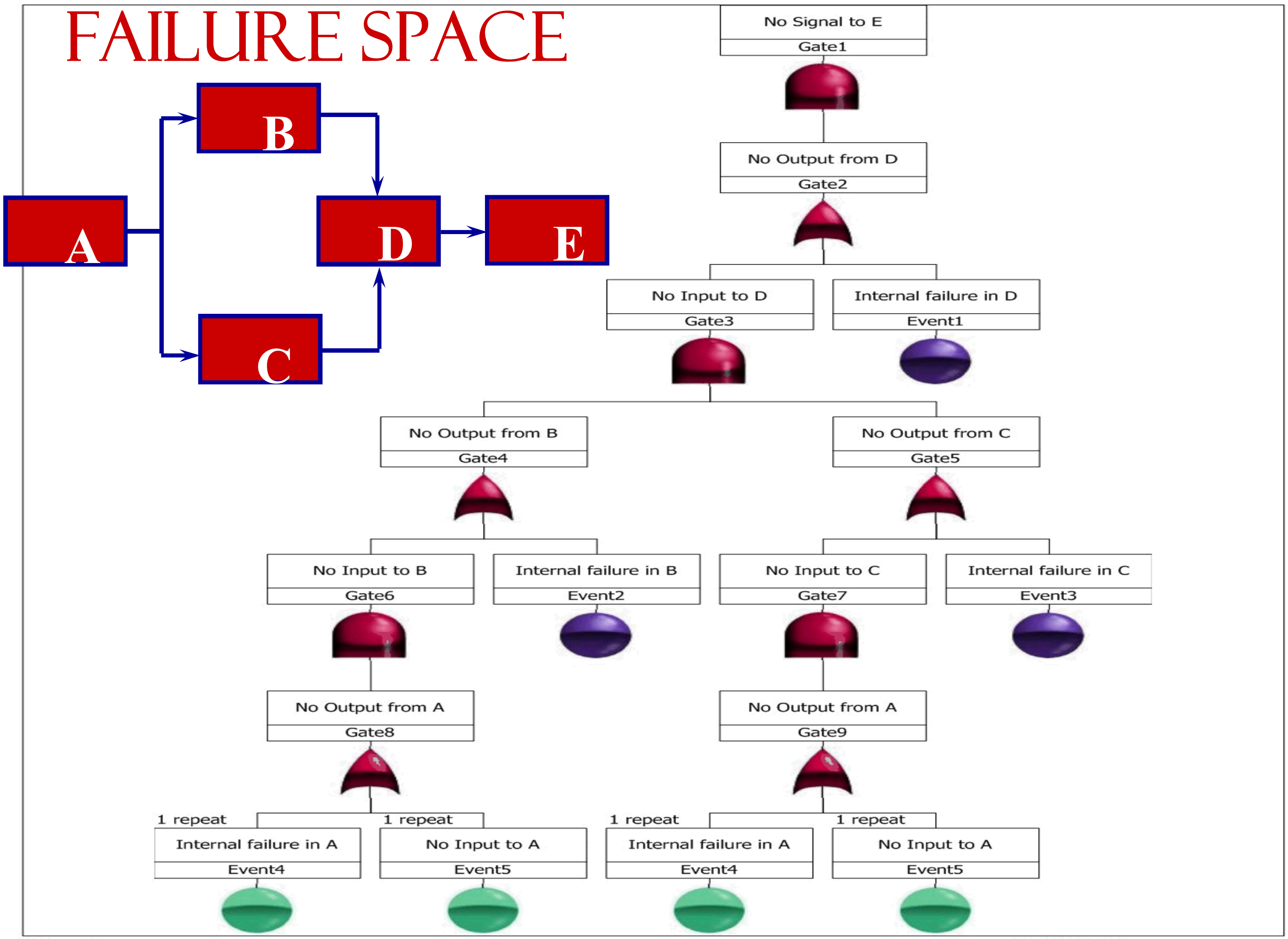
Success Space: An input signal to A provides an output to B and C. An output from B and/or C produces a signal from D which finally passes a signal to E.

Relex

Fault Tree Diagram

File Name: FTA Example 1.rfp

FAILURE SPACE



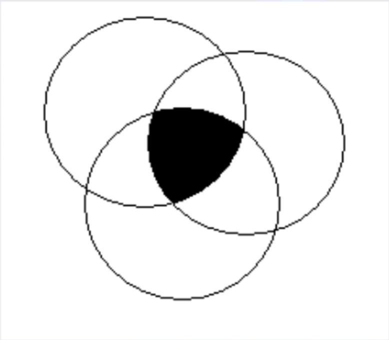
Print Date: 3/8/2011
Print Time: 1:06 PM

Set Theory / Boolean Algebra

- The software does this all for us
  - It’s been independently V&V’d
- I’ll breeze through this part just to let you know how it’s done.
  - Write Boolean equations
  - Substitute to get system equation
  - Reduce equations using theorems and identities
  - Find cut sets and their importance

SET THEORY

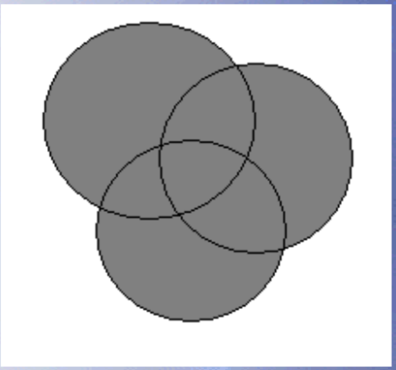
"Intersection" Operation



$X \cap Y \cap Z$

$X \bullet Y \bullet Z$

"Union" Operation



$X \cup Y \cup Z$

$X + Y + Z$

Operation	Probability	Mathematics	Engineering
Union	A or B	$A \cup B$	A + B
Intersection	A and B	$A \cap B$	A•B or AB

Fault Tree Cut Set Solution

Gate 1 = No Signal from E
Gate 2 = No Output from D
Gate 3 = No Input to D
Gate 4 = No Output from B
Gate 5 = No Output from C
Gate 6 = No Input to B
Gate 7 = No Input to C
Gate 8 = No Output from A
Gate 9 = No Output from A

Step 1: Generate one equation for each intermediate event in fault tree (eight intermediate events)

Gate1 = Gate2

Gate 2 = Gate 3 + Event 1

Gate 3 = Gate 4 • Gate 5

Gate 4 = Gate 6 + Event 2

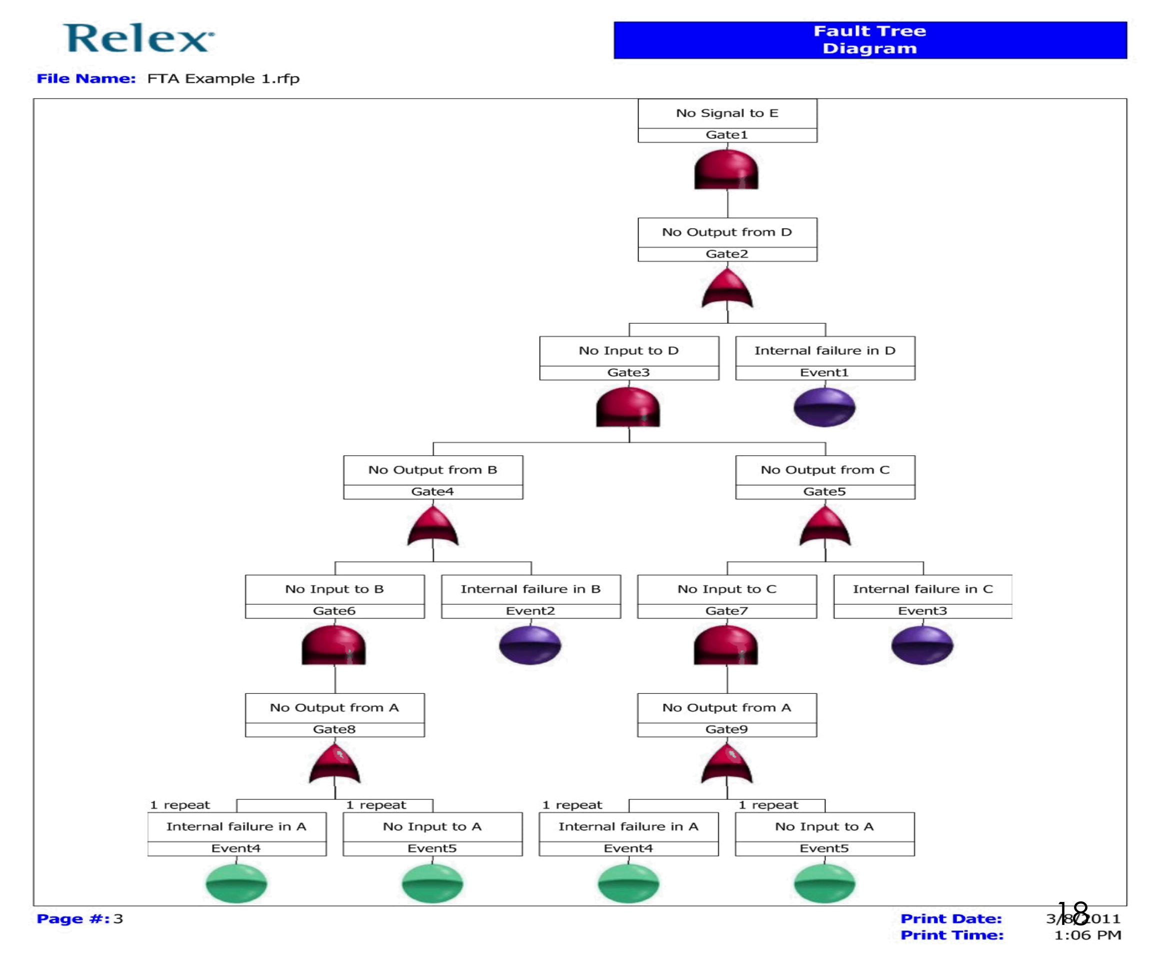
Gate 5 = Event 3 + Gate 7

Gate 6 = Gate 8

Gate 7 = Gate 9

Gate 8 = Event 4 + Event 5

Gate 9 = Event 4 + Event 5



Fault Tree Cut Set Solution (cont.)

Step 2: Generate the top event equation and substitute the equations that define the intermediate events

Gate 1 = Gate 2

= Gate 3 + Event 1

= (Gate 4 • Gate 5) + Event 1

= (Gate 6 + Event 2)•(Gate 7 + Event 3) + Event 1

= (Gate 8 + Event 2)•(Gate 9 + Event 3) + Event 1

= ((Event 4 + Event 5) + Event 2)•((Event 4 + Event 5) + Event 3) + Event 1

Fault Tree Cut Set Solution (cont.)

Step 3: Expand the equation using the distributive and associative laws:

Gate 1 = ((Event 4 + Event 5) + Event 2)•((Event 4 + Event 5) + Event 3) + Event 1
= (Event 4 + Event 5 + Event 2)•(Event 4 + Event 5 + Event 3) + Event 1
= Event 4•Event 4 + Event 4•Event 5 + Event 4•Event 3 + Event 5•Event 4 + Event 5•Event 5 + Event 5•Event 3 + Event 2•Event 4 + Event 2•Event 5 + Event 2•Event 3 + Event 1

Fault Tree Cut Set Solution (cont.)

Step 4: Minimize the expression using P • P = P and P + (P • Q) = P

- Cut sets reduced using P • P = P:
  - Intersection of a set with itself is the set
  - Union of a set with itself is the set

  Event 4 • Event 4 = Event 4

  Event 5 • Event 5 = Event 5

- Cut sets further reduced using P + (P•Q) = P; for example:
  - Union of set with a subset of that set is the set

  Event 4 + Event 4 • Event 5 = Event 4

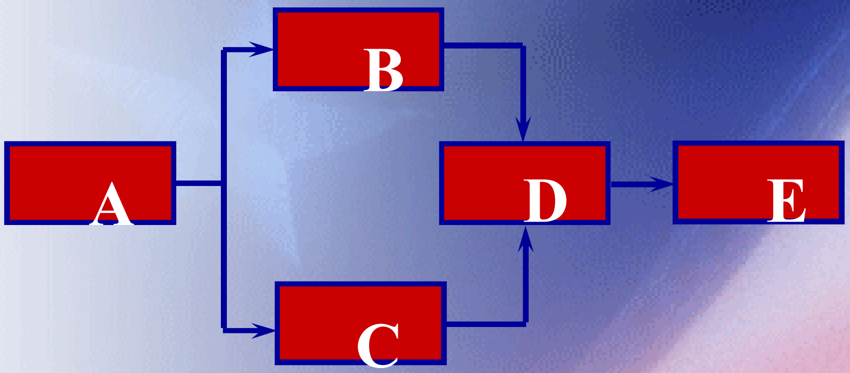
- Following reduction using identities, the minimal cut sets remain comprised of basic events

Example Fault Tree Cut Sets

Top Event Equation:

Gate 1 = Event 5 + Event 4 + Event 1 + Event 3 • Event 2.

Gate 1 = Event 5 OR Event 4 OR Event 1 OR (Event 3 AND Event 2)



Individual minimal cut sets:

Event 5	(No input to A)
Event 4	(Internal failure in A)
Event 1	(Internal failure in D)
Event 3 • Event 2	(Internal failure in B and Internal failure in C)

FAULT TREE MANUAL SOLUTION AND QUANTIFICATION

- Assigning the following basic event probabilities (no units specified):

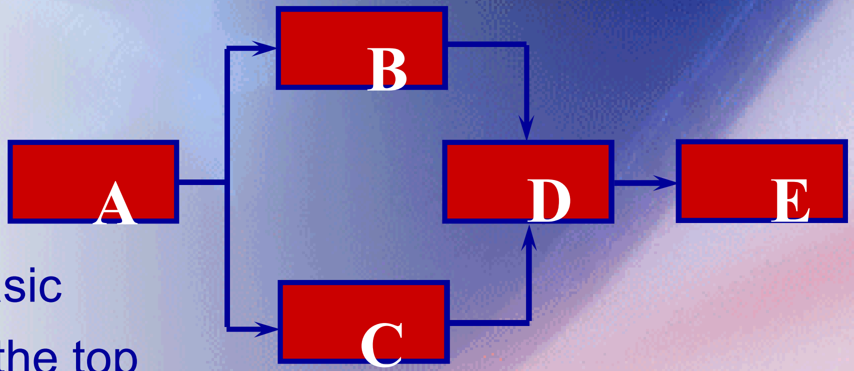
  Event 5 = 1E-4 (no input to A) 1/10000

  Event 4 = 5E-3 (Internal failure to A) 5/1000

  Event 2 = 1E-1 (Internal failure to B) 1/10

  Event 3 = 8E-3 (Internal failure to C) 8/1000

  Event 1 = 3E-3 (Internal failure to D) 3/1000



- Cut sets are quantified, assuming the basic event occurrences are independent, for the top event probability:

P(No signal to E) = 1E-4 + 5E-3 + 3E-3 + 1E-1•8E-3
= 8.9E-3

Cut Set Importance

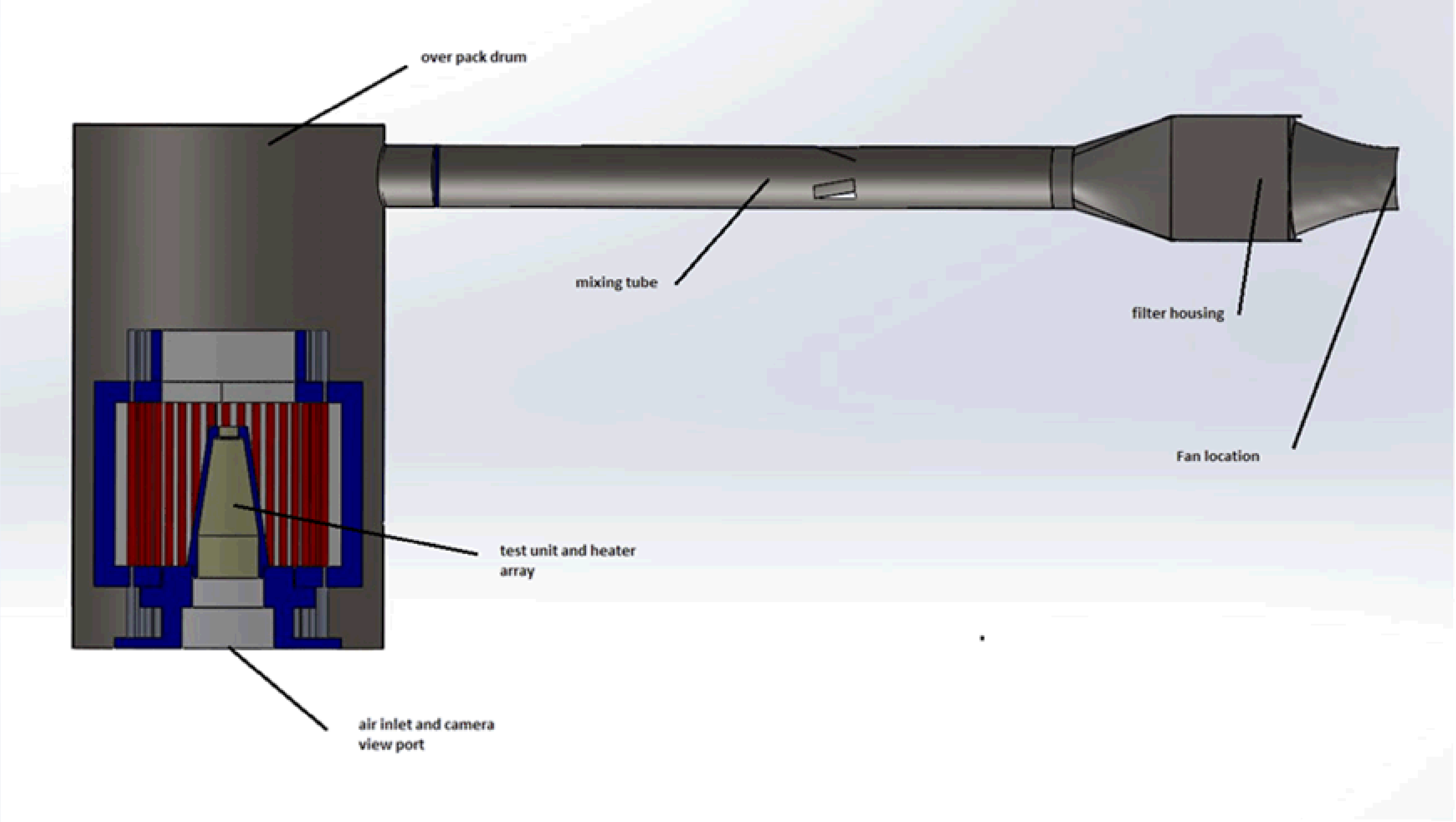
- Relative cut set importance is the ratio of the minimal cut set probability to the total system top event probability

Event 5 = 1E-4 (no input to A)
Event 4 = 5E-3 (Internal failure to A)
Event 2 = 1E-1 (Internal failure to B)
Event 3 = 8E-3 (Internal failure to C)
Event 1 = 3E-3 (Internal failure to D)

- Cut Set

Cut Set	Importance
Event 5 (No input to A)	1.1%
Event 4 (Internal failure in A)	56.2%
Event 1 (Internal failure in D)	33.7%
Event 3 • Event 2 (I.F. in B&C)	9.0%

Cone Thermal Test (Pre-FTA)



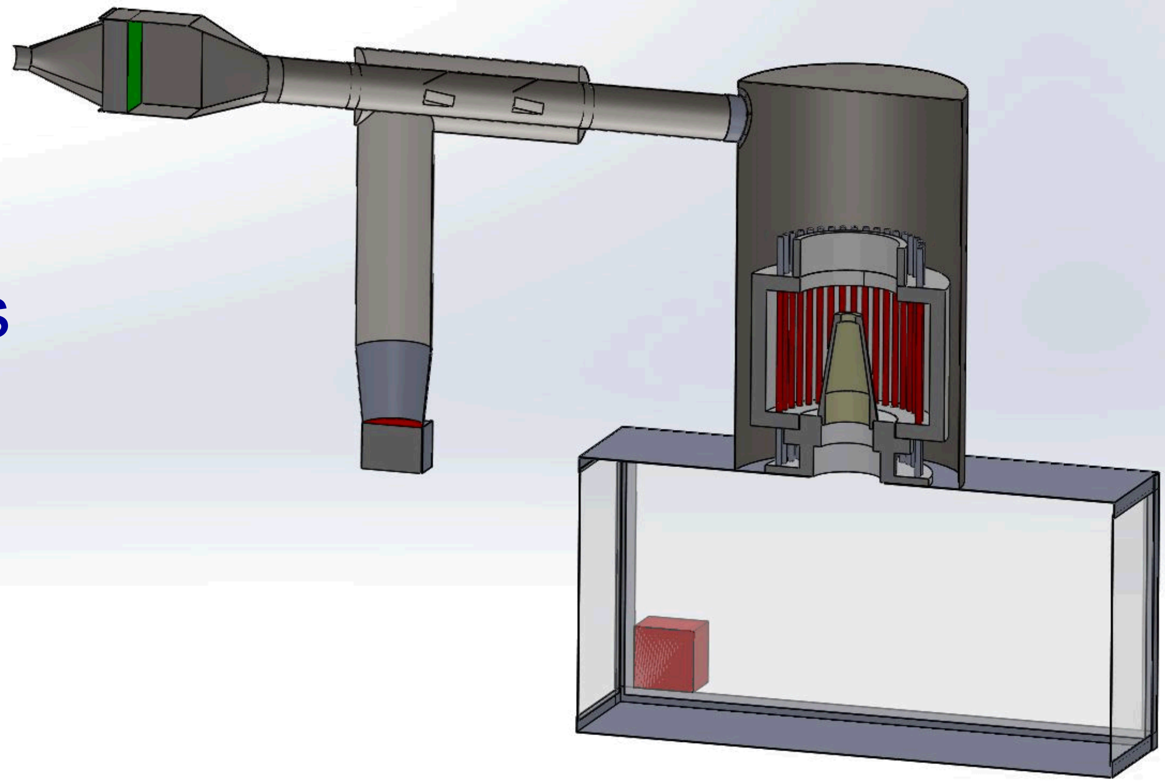
Asbestos release identified as one Unacceptable Consequence

Cutset Results:

- Several First-Order fault identified
  - Asbestos containment is fine only if everything works properly
  - Intended openings in the system are potential paths for release of asbestos
    - Air inlet at the bottom
    - Mixing ports to cool air prior to filter
  - Many possible fan faults could would force asbestos out of air inlet and mixing ports
    - Failure of power to fan (common at TTC)
    - Fan motor failure, shaft failure, etc.
  - Exit filter or seal failure
    - Mitigated by proper selection of filter, installation, and independent inspection by qualified contractor

Cone Thermal Test (Post-FTA)

- UPS added to fan system
- Mixing ports covered
- Air inlet covered



Engineered Safety / FTA Results

- FTA provided a formal method to evaluate the safety of the design and support the safety case
- First order faults / Single-point failures identified
  - Eliminated through redesign
  - Mitigated
    - Large design margins
    - Independently inspected
- Some second-order cutsets eliminated
  - Example: If both facility power and UPS fail, asbestos remains contained
- Initial FTA performed in one day. Redesign to eliminate issues done the day after
  - Test delayed by two weeks because of additional parts, assembly, and inspection
  - Lesson Learned: Have FTA done earlier rather than later
- FTA does not have to be labor intensive and is beneficial even for simple systems

RESOURCES

- Software:
  - PTC Windchill software
  - Isograph
  - INL's Saphire
  - Reliasoft
  - Itemsoft FTA
- Some provide trial versions
  - Limited time
  - Limited number of gates
  - Limited number of levels
- User groups
  - Poor customer service on the few I've used