

Medtronic Tempe Campus Design, Reliability and Manufacturability Design For Six Sigma

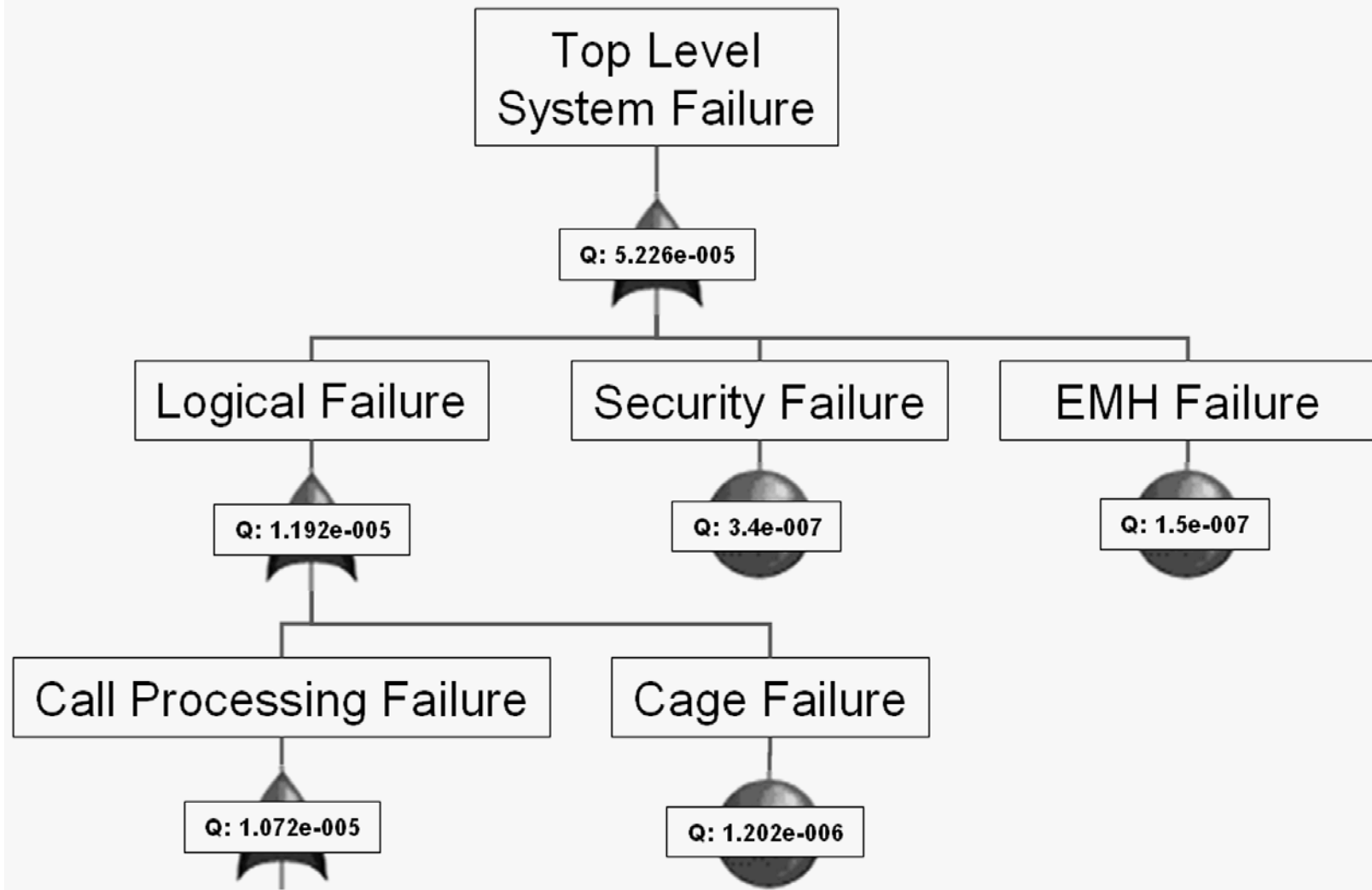


Medtronic Tempe Campus Introduction to Fault Tree Analysis (FTA)

Description of Fault Tree Analysis

- FTA provides qualitative analysis of cause-effect relationships for failures.
- If probabilities are known for lower level events, FTA can be used to calculate the probability of the top level failure.
(example on next slide)
- Fault trees can be simplified using Boolean algebra.

Example: FTA with Probabilities



History of Fault Tree Analysis

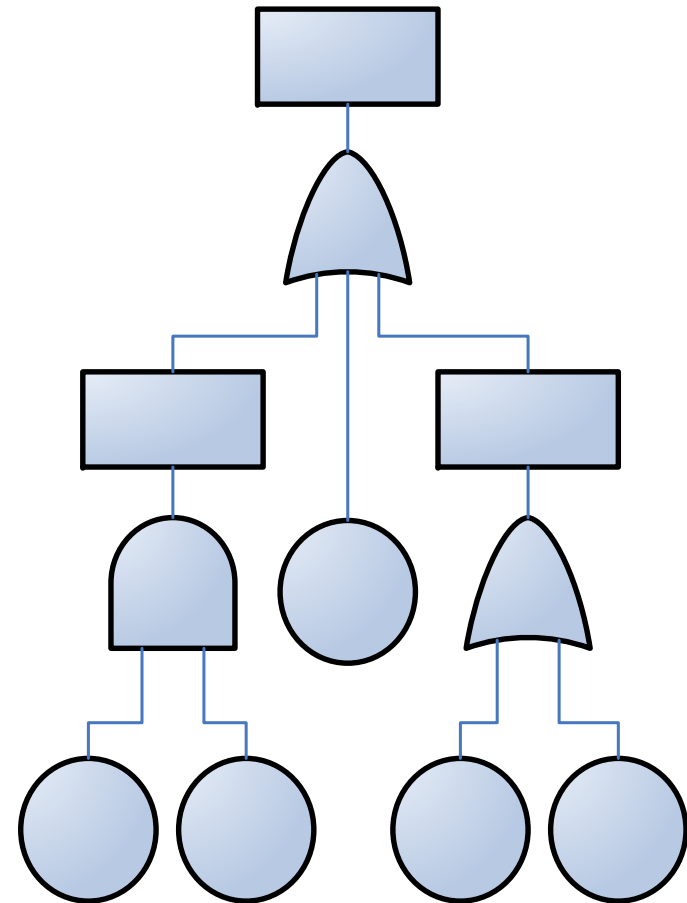
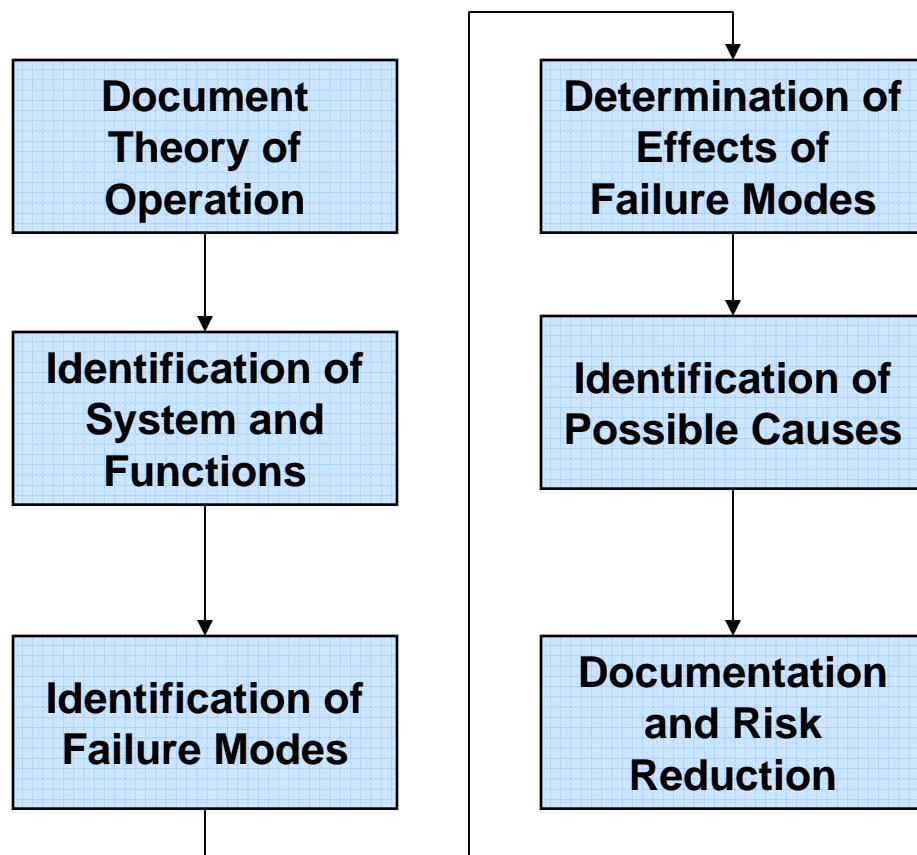
- FTA was first used by Bell Labs in the safety analysis of the Minuteman missile launch control system (1962).
- Later adopted and used by Boeing
- FTA has been applied in analyzing complex systems to improve reliability and safety and to develop diagnostic tools

Who Should Participate In FTA?

- Recommended membership for the FMEA team:
 - Project Manager
 - Design Engineer (hardware/software/systems)
 - Test Engineer
 - Reliability Engineer
 - Quality Engineer
 - Failure Analysis Engineer
 - Field Service Engineer
 - Manufacturing/Process Engineer
 - Safety Engineer

Preparation for Conducting FTA

FMEA → → → → then FTA





Updating FTA

- FTA and DFMEA are living documents
- Major changes (like system design change) require review and update
- Reliability projections should be refreshed

Customers for FTA


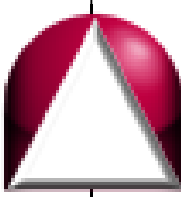
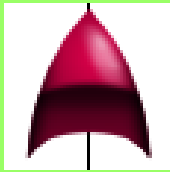
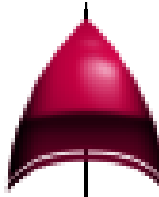
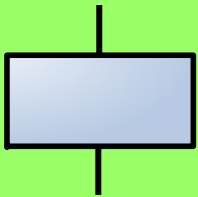
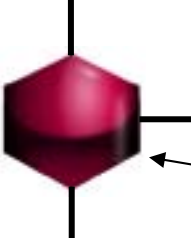
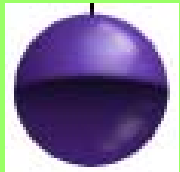
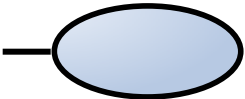

- Systems engineers
- Subsystem design engineers
- Reliability engineers
- Service and support engineers and technicians
- Failure Analysis engineers and technicians
- Safety analysis specialists
- Regulatory specialists

Assumptions

- Non-repairable system
- Markov process \leftrightarrow Exponential Reliability Model
 - Constant fault rates, $\lambda = 1/\text{MTBF}$
 - Future state depends only on present state and not on history – memoryless
 - Each system element is in one of two mutually exclusive states – failed or not failed

Symbols Commonly Used in Fault Trees

Note: This list of symbols is not comprehensive.

	<p>AND Gate If all input events occur, the output event will occur</p>		<p>Priority AND Gate Output event occurs if all events occur in the right order from left to right</p>
	<p>OR Gate If any input event occurs, the output event will occur</p>		<p>Exclusive OR Gate Output event occurs if one, but not both of the two input events occurs</p>
	<p>Event Any higher level event that is a result of lower level events</p>		<p>Inhibit Gate Input produces output when conditional event occurs</p>
	<p>Basic Event The lowest level event. The limiting resolution in our analysis.</p>	 	<p>Conditional Event Used with inhibit gate</p> <p>Sequence-Enforcing Gate Input events must occur in the left-to-right order</p>

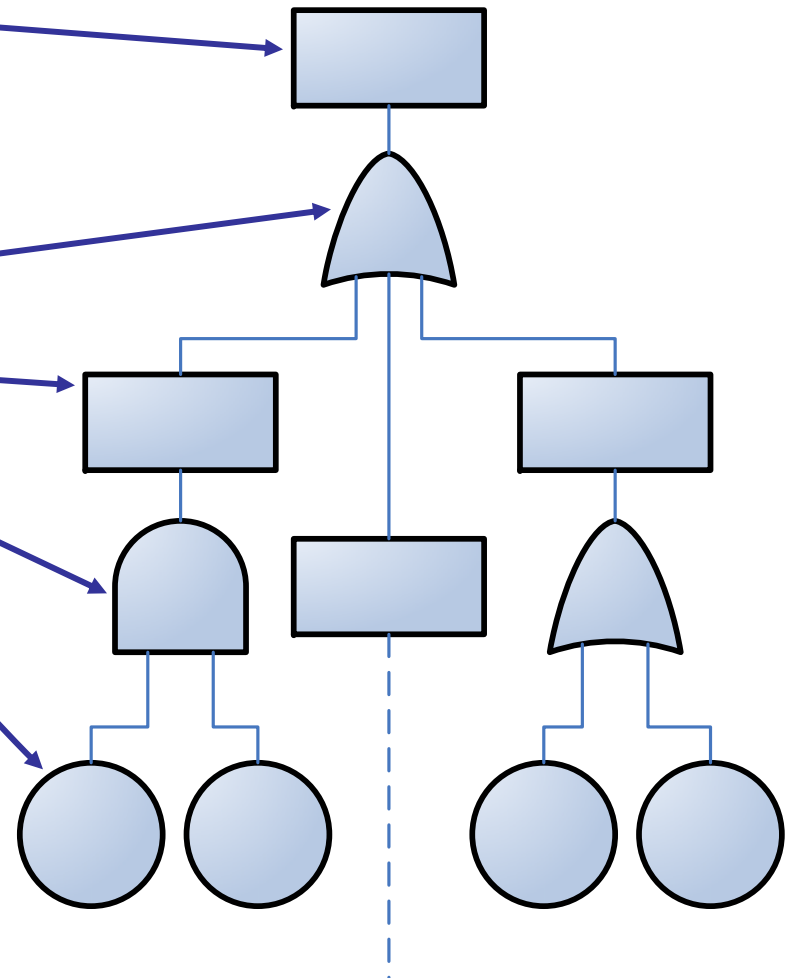
Mathematically equivalent to AND Gate

FTA Terminology

- **TOP event** – failure or loss at the top of the fault tree that is caused by lower level events
- **Lower level contributors** – Events below the top level that contribute to failure or loss at the top
- **Basic contributors** – As low as we choose to go when drilling down for lower level causal events
- **Cut set** – A set of events which, if they all occur, will cause the TOP event
- **Minimal cut set** – a cut set such that if any item is removed from the list, the system will no longer fail

Steps to Perform Fault Tree Analysis

1. Identify Undesirable TOP event
2. Establish the boundaries of the FTA
3. Construct the fault tree, starting with the primary event and working downward
4. Link contributors to TOP using logic gates
5. Identify first level contributors
6. Link second-level contributors to TOP using logic gates
7. Identify basic contributors
8. Analyze the fault tree to identify ways of eliminating events that lead to failure
9. Prepare a corrective actions and contingency plans for preventing and/or dealing with failures
10. Implement the plans
11. This is iterative – return to step one



P.L. Clemens, *Fault Tree Analysis*, Jacobs-Sverdrup, 4th Ed. February 2002

FTA – Best Practices

- Defining failure
 - Be very specific and consistent in defining failure events throughout the fault tree
 - Specify what fails and how it fails

Examples:

- Motor fails to start when start signal is input to relay 102-a
- Diagnostic test instrument produces negative result when positive reference sample is analyzed

FTA – Best Practices

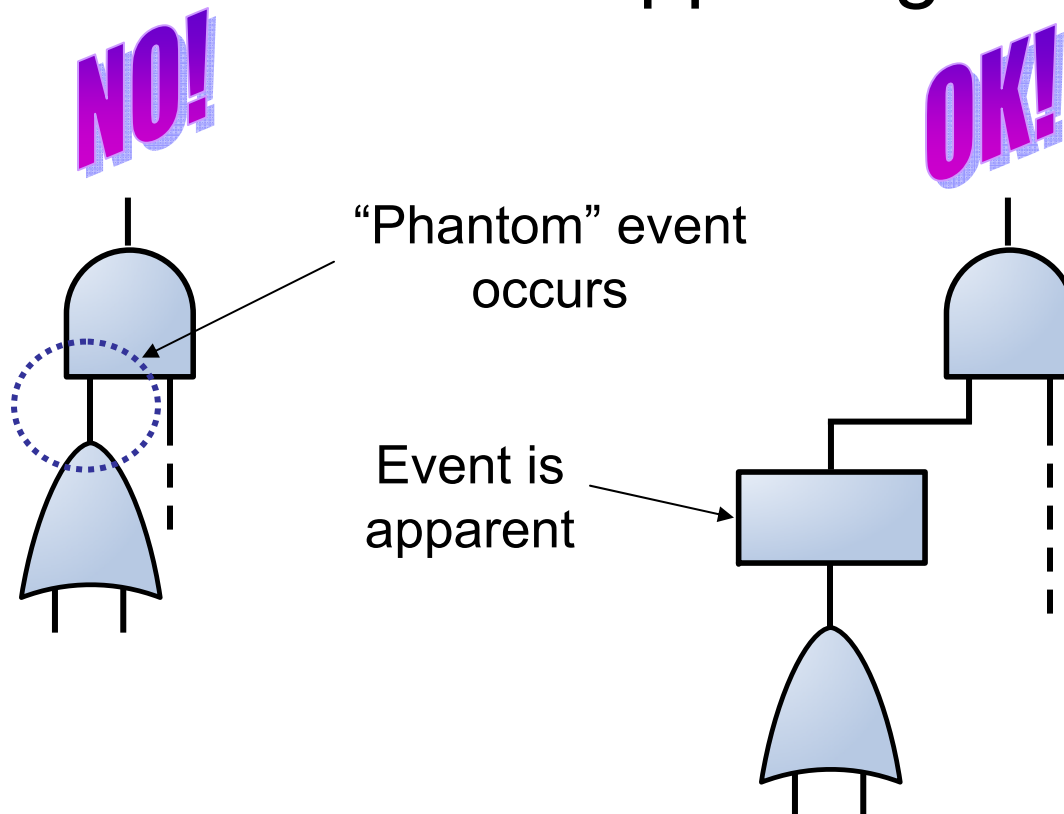
- Don't assume “a miracle occurs” that compensates for or mitigates a failure

Examples:

- A sudden downpour extinguishes the fire caused by knocking over the pot of boiling oil while deep frying a turkey on your deck
 - The F-18 makes a low approach and is about to hit the fantail of the carrier but a gust of wind provides the necessary lift to allow a safe landing
- All faults at the input to a gate must be statistically independent
- Faults can appear at multiple points in the tree, but not as inputs to the same gate

FTA – Best Practices

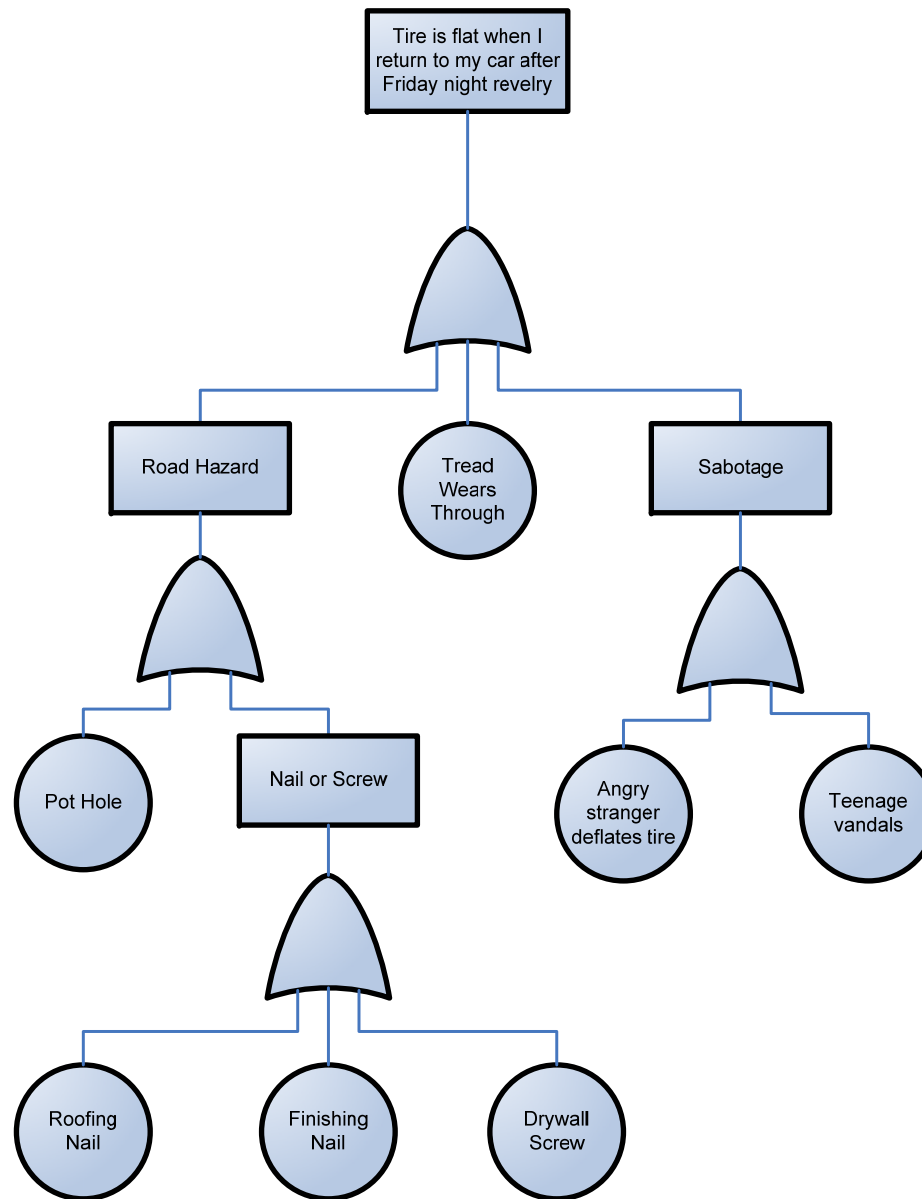
- Don't connect the output of one gate directly to the input of another as it obscures what's happening.



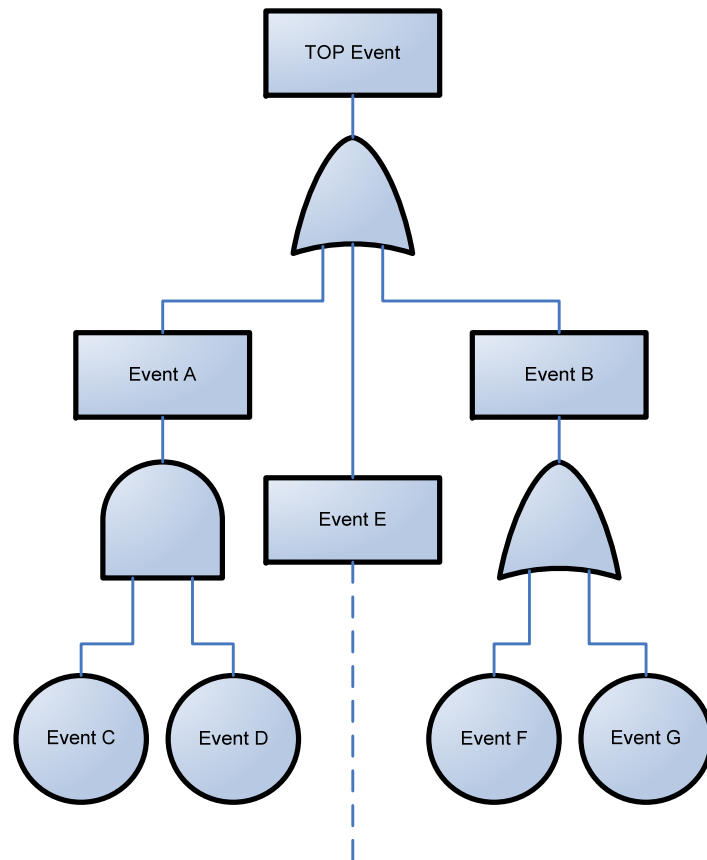
FTA – Best Practices

- TOP events must be well defined and specific
 - Examples:
 - Pressure vessel ruptures
 - First stage disk in jet engine rotor fractures during operation
 - Vehicles collide at particular intersection
 - Parachute fails to open
 - Missile misses target
 - Bird flu pandemic occurs
 - Medical diagnostic instrument produces false positive test result

A Simple Fault Tree Example



Example: Using Fault Trees to Calculate Probably of Failure



$$P(\text{TOP}) = P(A \text{ OR } B \text{ OR } E) \quad (1)$$

$$P(A) = P(C \text{ AND } D) \quad (2)$$

$$P(A) = P(C)P(D) \quad (3)$$

$$P(B) = P(F \text{ OR } G) \quad (4)$$

$$P(B) = P(F) + P(G) - P(F)P(G) \quad (5)$$

$$P(\text{TOP}) = P(A) + P(B) + P(E) - P(A)P(B) - P(A)P(E) - P(B)P(E) - P(A)P(B)P(E) \quad (6)$$

Substitute (3) and (5) into (6) to get expression for $P(\text{TOP})$

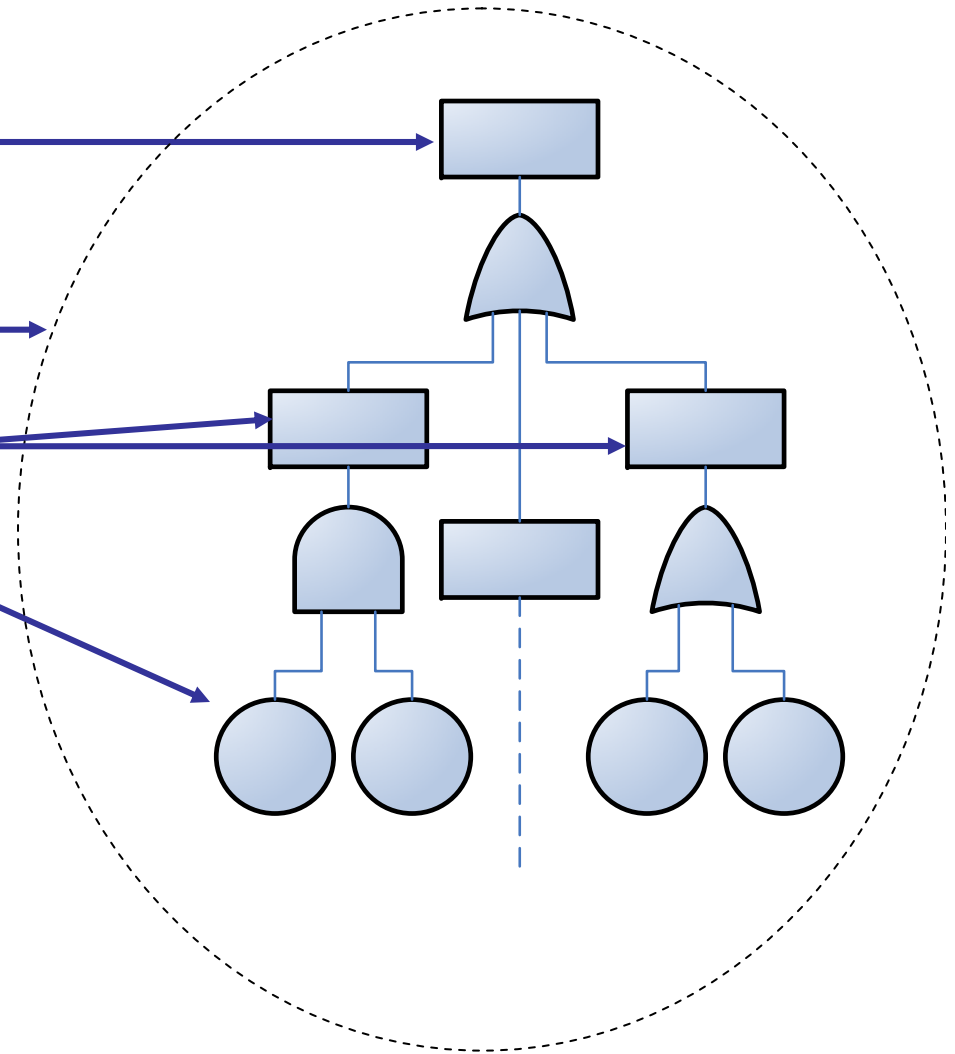
Team Activity: Lamp Example

I have a lamp on my desk. The lamp is plugged into an outlet controlled by a wall switch. I usually leave the lamp switch in the “on” position and turn the lamp on or off using the wall switch when I enter or leave the room. One evening, I flip the wall switch from “off” to “on” and the light doesn’t turn on. What are the events that could lead to that failure and how does the Fault Tree look ?

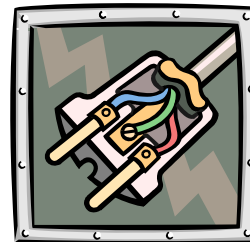
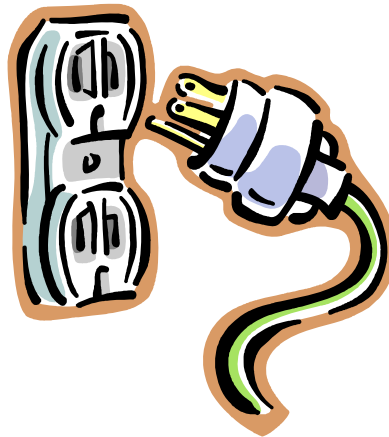
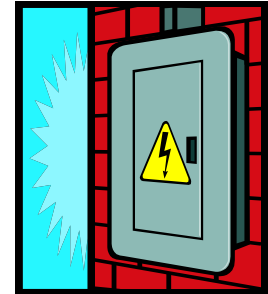
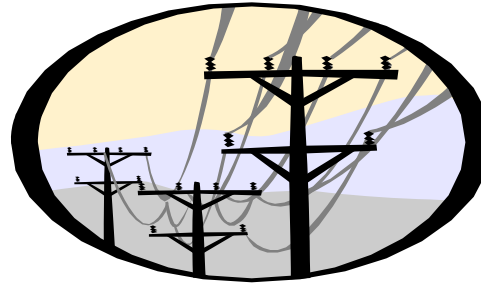
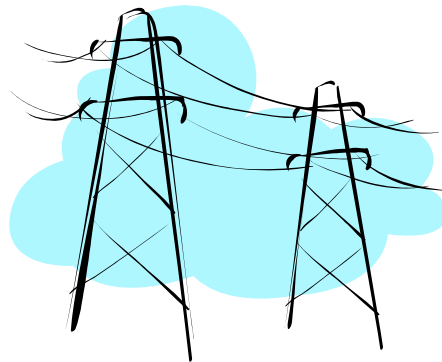


Aspects to Define

- Top event corresponding to failure or loss
- What to include in the analysis
- First level contributors
- The basic contributors
- How the events combine to cause failure



What to include (or exclude) in the analysis...



Team Exercise

Develop The Fault Tree for
the Lamp



Exercise: Fault Tree Analysis

- Objective
 - To practice developing and analyzing a Fault Tree
- Instructions
 - Break into 4-5 person teams
 - Select a system or subsystem your team is familiar with from your current project
 - Develop a Fault Tree
 - Identify 1 or 2 undesirable top level events – these are the failure conditions being analyzed
 - Construct the fault tree, starting with the primary event and working downward
 - Establish the boundaries of the FTA – what to include in the analysis
 - Analyze the fault tree to identify ways of eliminating events that lead to failure
 - Be prepared to present your results to the class
- Time: 45 minutes

References

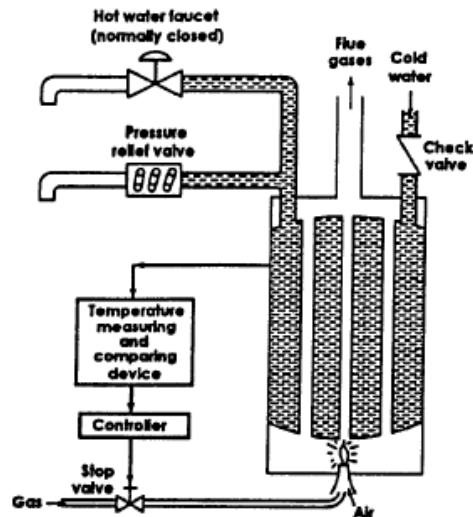
- P. L. Clemens, Fault Tree Analysis, Jacobs-Sverdrup, 4th Ed. February 2002
- Marvin Rausand, System Reliability Theory, 2nd Ed., Wiley, 2004
- W. E. Vesely, F. F. Goldberg, N. H. Roberts, D. F. Haasi, Fault Tree Handbook, U.S. Nuclear Regulatory Commission, NUREG-0492, January 1981
- J. D. Andrews, T. R. Moss, Reliability and Risk Assessment, 2nd Ed., ASME Press
- P. L. Clemens, A Charlatan's Guide to Quickly Acquired Quackery: The Trouble With System Safety, Presentation to NASA Safety Training Center, 2001

Optional Exercise – FMEA and FTA for Hot Water Heater

FMEA Exercise: Perform a Design Failure Mode & Effects Analysis on the hot water heater system.

Deliverables:

- List of basic and/or secondary function(s) of the water heat.
- List at least two failure modes.
- Create a FMEA cause-and-effect diagram for one of the failure mode.
- Identify at least 4 complete rows that include a failure effect/ failure mode/ cause (note: you may use a cause or effect for more than failure).
- Based on your FMEA, which concern(s) should be addressed first?
- Briefly discuss how you might resolve your concern?



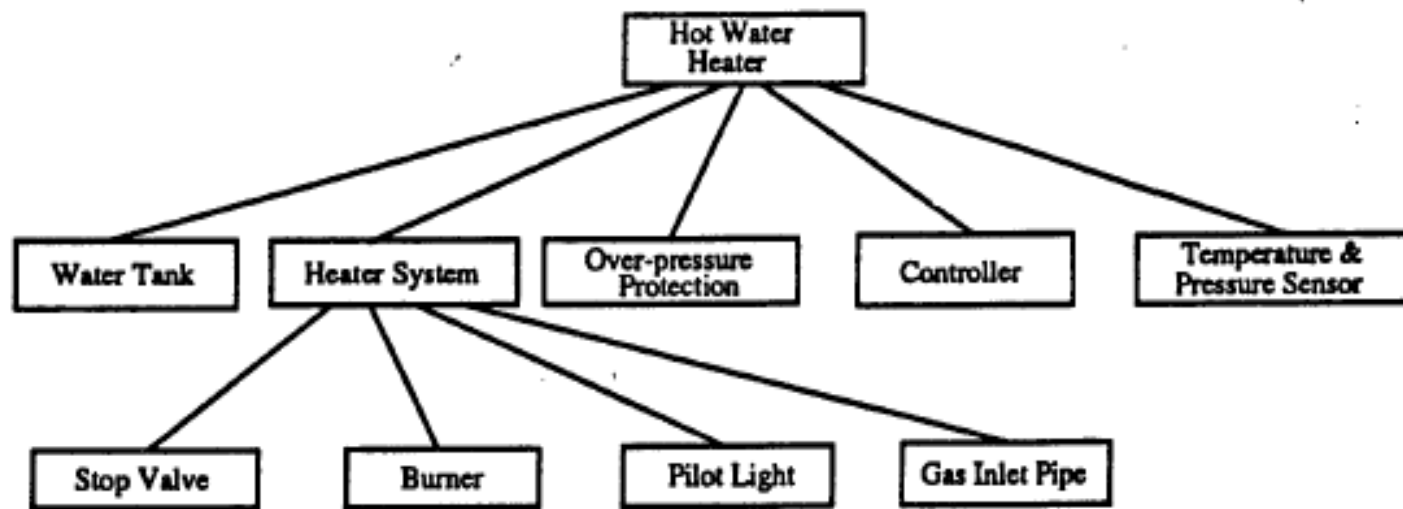
Hot Water Heater schematic

The functions of the system components are:

Component	Function
stop valve	controls gas flow; full-on/full-off (controlled by the controller)
controller	opens and closes stop valve (responds to temperature sensor)
pressure/temp. sensor	senses water pressure & temperature
check valve	prevents reverse flow if over-pressure
relief valve	opens when pressure > 100 psig
pilot light	lights burner (always on)
burner	heats water (operated by stop valve)
tank	holds water (safe up to 100 psig)
faucet	releases water when needed

Optional Exercise – FMEA and FTA for Hot Water Heater

FMEA Exercise: Perform a Design Failure Mode & Effects Analysis on the hot water heater system.



Hierarchical representation of the hot water heater and its subsystems

Relax FMEA

TECHNICAL HIGHLIGHTS

Supported FMEA Types

- › Process
- › Design
- › Functional
- › Component
- › Automotive
- › Piece-part

Supported Standards

- › MIL-STD-1629A
- › FMD-97
- › BS5760
- › HAZOP
- › SAE ARP5580
- › AIAG
- › SAE J1739
- › Ford
- › GM
- › Daimler-Chrysler
- › IEC 60812

Supported Calculations

- › Mode failure rates
- › Criticality
- › Risk priority number (RPN)
- › Risk level
- › Percent isolation
- › Percent detection
- › User-definable

Failure Mode Libraries

- › FMD-97
- › FMD-91
- › MIL-HDBK-338
- › NPRD3
- › RADC-TR-84-244
- › RADC-TR-844 4-A

Data Hierarchy

- › Mode Only
- › Single effect per mode
- › Multiple effects per mode
- › Multiple effects per cause
- › Multiple causes per effect

Interface Types

- › Windows
- › Web, zero-client

Specialized Formatting

- › Background color
- › Text color
- › Font style
- › Font size
- › Marked cell
- › Notes

Analysis Outputs

- › Standard formats per specifications
- › Criticality matrices
- › Risk levels
- › Failure likelihood rank
- › Top (n) failure modes by RPN
- › Failure modes and effects summary
- › Top (n) failure modes by mode criticality
- › Action item list
- › Failure mode cause Pareto

Data Linkages

- › Event Tree
- › Fault Tree
- › FMEA
- › RBD
- › OpSim
- › Reliability Prediction

Import/Export Formats

- › Microsoft Excel
- › Microsoft Access
- › Text
- › LSAR

Graph Types

- › Area
- › Bar
- › Line
- › Pareto
- › Pie
- › Scatter
- › Stacking bar

Report Formats

- › Microsoft Word
- › Microsoft Excel
- › Adobe PDF
- › RTF
- › HTML

Databases Supported

- › Microsoft SQL Server
- › Oracle
- › Microsoft SQL Server Desktop Engine (MSDE)
- › Microsoft Jet Engine (Access compatible)

Enterprise Modules

- › Administrator
- › Audit trail
- › Alerts
- › iArchitect
- › Dashboard

Available Services

- › Software module training
- › Theory training
- › Professional consulting services
- › Web-based RETAIN (online training) sessions
- › Expert technical support
- › Online customer support center

Relex - [Laser Cutter, System: Laser Cutter]

File Edit View Insert Tools System FMEA Records Window Help

FMEA - System Tree

Part/Assembly Name	Description	System Tree ID
Laser Drive System	Laser Drive and Positioning	SYS-022
Primary Slide Bearing	1/4 Inch Stainless Steel Traversing Beam Bearing	SYS-023
Drive Belt	X-Axis Laser Drive Belt	SYS-024
Rotary Drive Motor	45LB5(IN-LB5) Peak Torque Drive Servo	SYS-025
Pulley	50mm Axis Drive Pulley	SYS-026

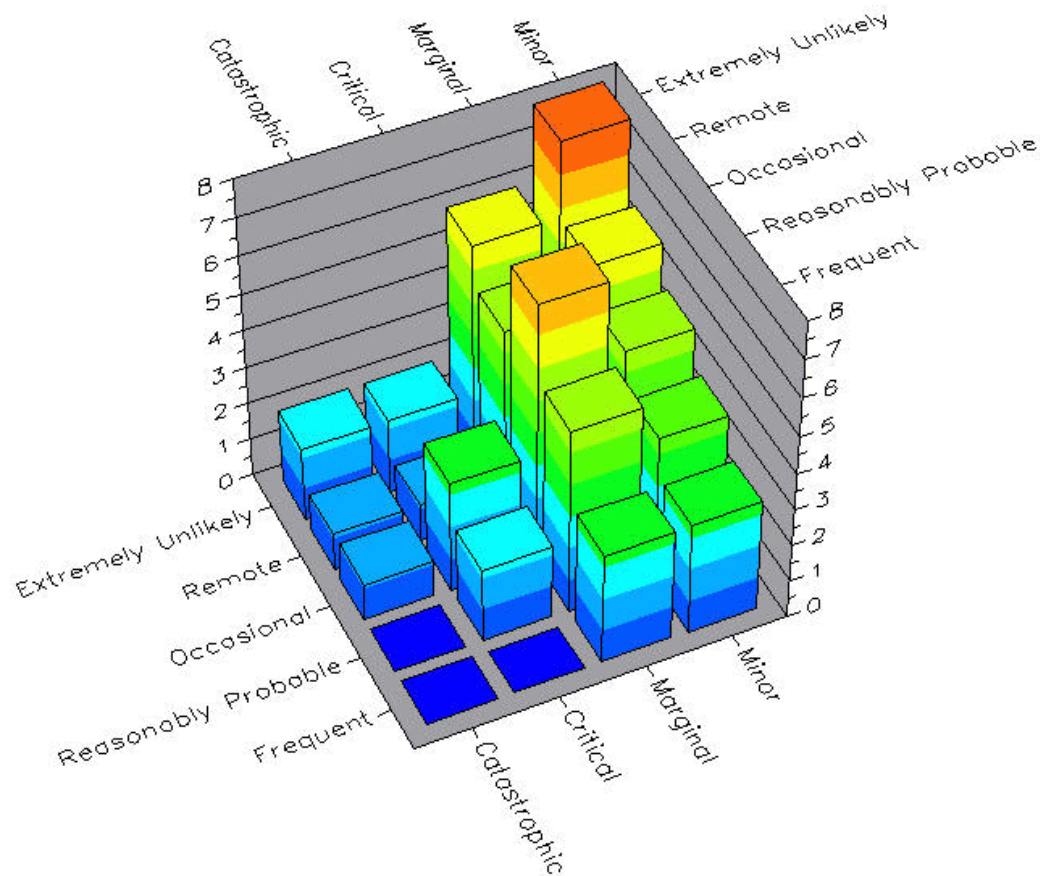
System Tree Configuration Table FMEA List FMEA - System Tree

FMEA Table

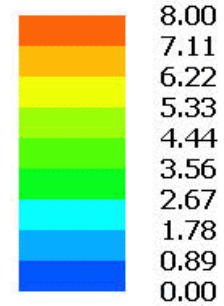
	Item/Function	Failure Rate	Failure Mode	Mode %	Mode Failure Rate	Local Effect	Next Effect	End Effect	Severity	Occurrence	Cause(s) of Failure
117	Primary Slide Bearing	67	Jammed	30	20	Cannot Move on Axis	Metal is not cut	Machine Downtime	Marginal	Remote	Contamination
Lubrication Problem											
119			Restricted	70	47	Cannot Freely Move on Axis	Metal is not cut correctly	Machine Downtime, Loss of Product	Marginal	Reasonably Probable	Contamination
Lubrication Problem											
121	Drive Belt	29	Breaks	90	26	Cannot support or move the laser	Metal is not cut	Machine Downtime	Critical	Occasional	Defective Wear
122			Loose	10	3	The laser cannot be moved correctly	Metal is not cut	Machine Downtime	Minor	Extremely Unlikely	Overstressed
123			Inoperative	30	2	Cannot Move on Axis	Metal is not cut	Machine Downtime	Marginal	Extremely Unlikely	Contamination
124											Lubrication Problem

Ready FPMH FMEA 121 of 144

FMEA Criticality Matrix



Legend



Linked to Fault Tree Analysis

Relex - [Garage Door Opener, System: Garage Door Opener]

File Edit View Tools System Event Tree Window Help

Event Tree Results

Branch Number	Branch	Sequence	Consequence	Frequency	Unavailability	Unreliability	Availability	Reliability
1	Branch10	EP-CS	Obstacle injured/damaged minimally	3.903900e-007	3.468750e-009	0.000499	1.000000	0.999501
2	Branch12		Closing garage door stops per power failure	0.005882	0.001000	0.001000	0.999000	0.999000
3	Branch16	EP	Obstacle crushed by closing garage door	0.000006	9.394531e-018	1.947183e-007	1.000000	1.000000
4	Branch8	EP-NC	Obstacle not injured/damaged by closing garage door	5.000000e-007	0.999000	0.998501	0.001000	0.001499

Event Tree Diagram

Obstacle in path of closing door: Branch1: Failure

Electric power available: Branch2: Success

Electric power failed: Branch3: Failure

Non-Contact Safety Reverse Working: Branch4: ... Branch8: Null

Non-Contact Safety Reverse Failed: Branch5: Fa...

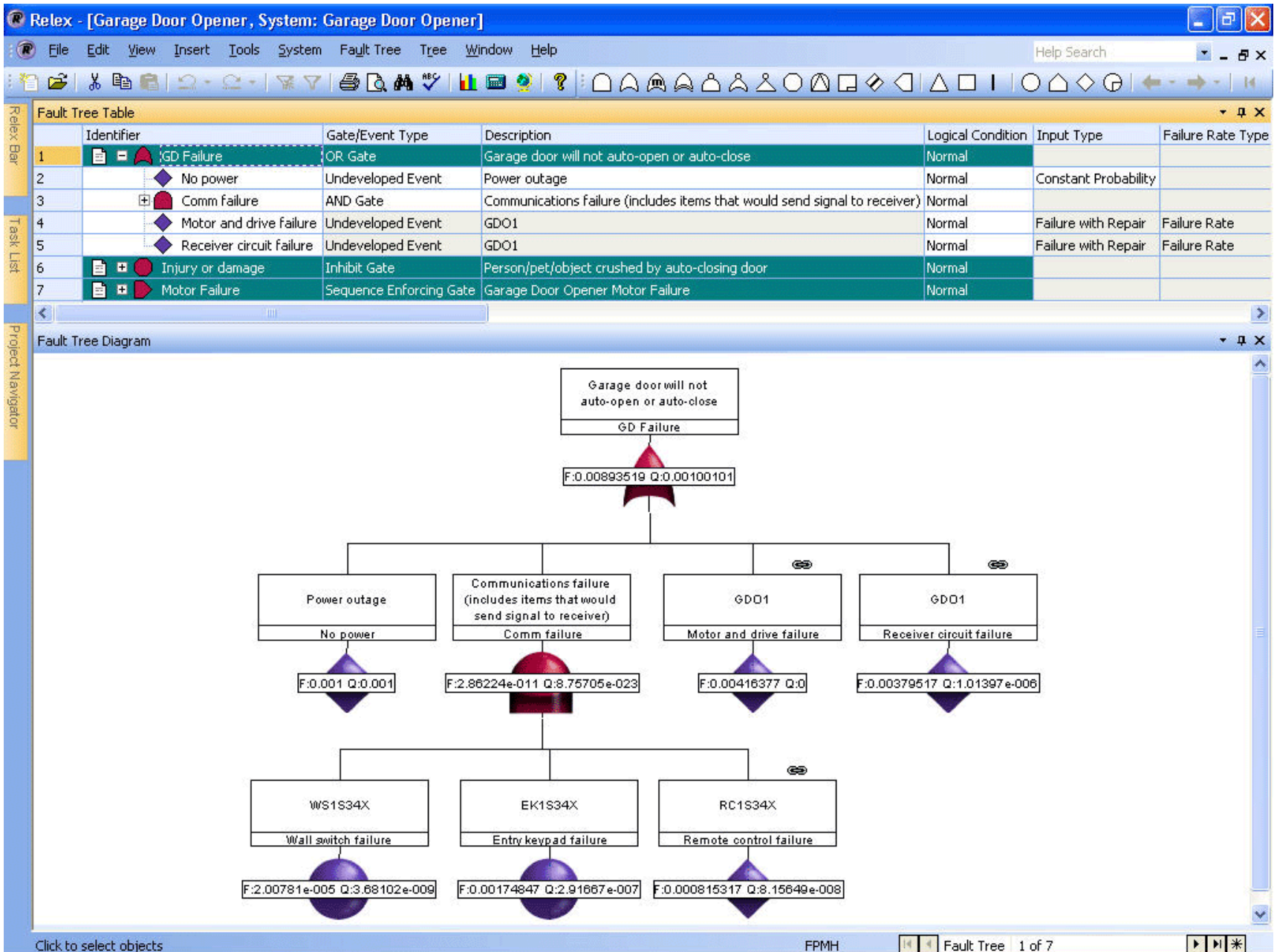
Branch6: Null

Contact Safety Reverse Working: Branch10: Su...

Contact Safety Reverse Failed: Branch16: Failure

Branch12: Null

Ready FPMH Event Tree Branch Calculation Results





TECHNICAL HIGHLIGHTS

Static Gate Types

- › AND
- › OR
- › Voting
- › XOR (Exclusive OR)
- › NAND
- › NOR
- › NOT
- › Inhibit
- › Transfer
- › Remarks
- › Pass-through

Dynamic Gate Types

- › Priority AND
- › Functional dependency
- › Sequence enforcing
- › Spare

Event Types

- › Basic
- › Spare
- › House
- › Undeveloped
- › Conditional

Importance Measures

- › Birnbaum
- › Criticality
- › Fussell-Vesely

Common Cause Failures

- › Beta
- › MGL
- › Alpha
- › BFR

Calculation Methods

- › Cut set summation
- › Cross product
- › Esary Proschan
- › Exact
- › Qualitative
- › Quantitative

Supported Calculations

- › Unreliability
- › Unavailability
- › Frequency of failures
- › Number of failures
- › Cut sets
- › Importance measures

Fault Tree Views

- › Graphical
- › Tabular

Analysis Outputs

- › Graphical diagram
- › Event importance
- › Minimal cut sets
- › Unreliability/reliability vs. time
- › Unavailability/availability vs. time
- › Gate/event results
- › Failure frequency vs. time

Data Linkages

- › Event Tree
- › Fault Tree
- › FMEA
- › Markov
- › Reliability Prediction

Import/Export Formats

- › Microsoft Excel
- › Microsoft Access
- › Text

Report Formats

- › Microsoft Word
- › Microsoft Excel
- › Adobe PDF
- › RTF
- › HTML

Databases Supported

- › Microsoft SQL Server
- › Oracle
- › Microsoft SQL Server Desktop Engine (MSDE)
- › Microsoft Jet Engine (Access compatible)

Enterprise Modules

- › Administrator
- › Audit trail
- › Dashboard

Available Services

- › Software module training
- › Theory training
- › Professional consulting services
- › Web-based RETAIN (online training) sessions
- › Expert technical support
- › Online customer support center



A fault tree analysis is generally much faster to perform than a FMEA, but it is much more targeted. A fault tree is most effective when an undesired event or top event is what needs to be analyzed, while a FMEA is much broader. FMEA terms such as failure mode and end effect can be equated to fault tree terms such as basic event and top event. Taking a given FMEA end effect, a fault tree may be created with the top event of the fault tree being the same as the FMEA end effect.

Note: One limitation of FMEAs is that all failures are assumed to be mutually exclusive and not dependent on each other. This is in contrast to standard fault trees where certain events may all need to occur to cause the top event to occur, i.e. those that are joined using AND gates.

Relex provides a function in the FMEA module that allows you to automatically create a fault tree from the final results of your FMEA.

Select Project>Build Fault Tree from FMEA main menu option to build a fault tree from your FMEA. Select from the list of end effects and mission phases from which to build the fault tree. The selected end effect becomes the top event in the fault tree. If the option "Prune branches with no events" is enabled, Relex does not include fault tree branches that contain no events.

Relex automatically creates a fault tree with a top event, OR gates, and basic events representing the failure modes in the FMEA.

Once the fault tree has been created, the link with FMEA is complete. From this point forward, any changes made to the fault tree do not effect the FMEA. Similarly, changes to the FMEA do not effect the fault tree.

© Relex Software Corporation