Saving Millions with Fault Tree Analysis

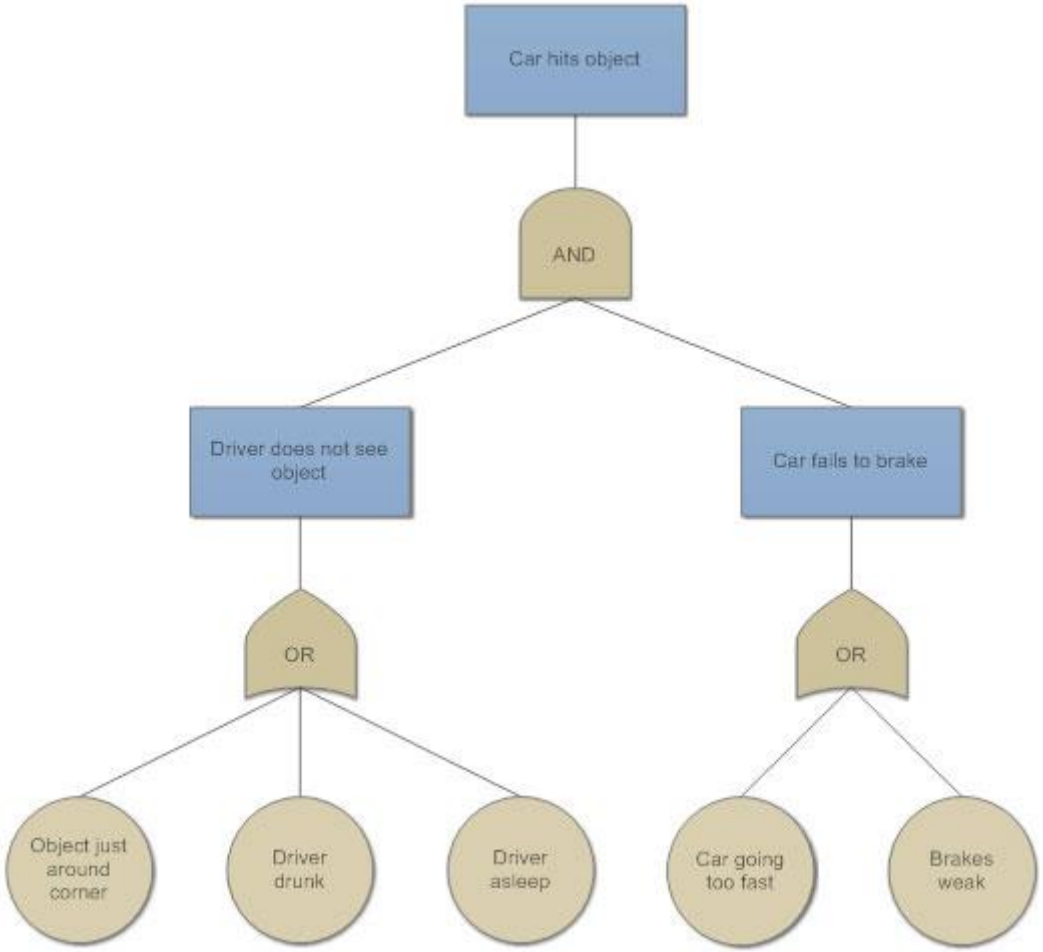
- Who has used Fault Tree Analysis (FTA) / In what industry was it used?

- My thesis is that FTA is greatly underutilized, and
  this is costing companies many $M / costing industry many $B.

Let’s start with . . . What is Fault Tree Analysis?

So . . . What is Fault Tree Analysis?

- FTAs were originally developed in 1962 at Bell Laboratories by H.A. Watson
  - Traditionally used to analyze reliability or safety.
  - Also useful for success planning and mitigating inadequate design records.
- IEC 61025 standardizes FTA language
  - IEC 61025, section 5.3:
    The fault tree is particularly suited to the analysis of complex systems comprising several functionally related or dependent subsystems with different performance objectives.
    This is especially true whenever the system design requires the collaboration of many specialized technical design groups.



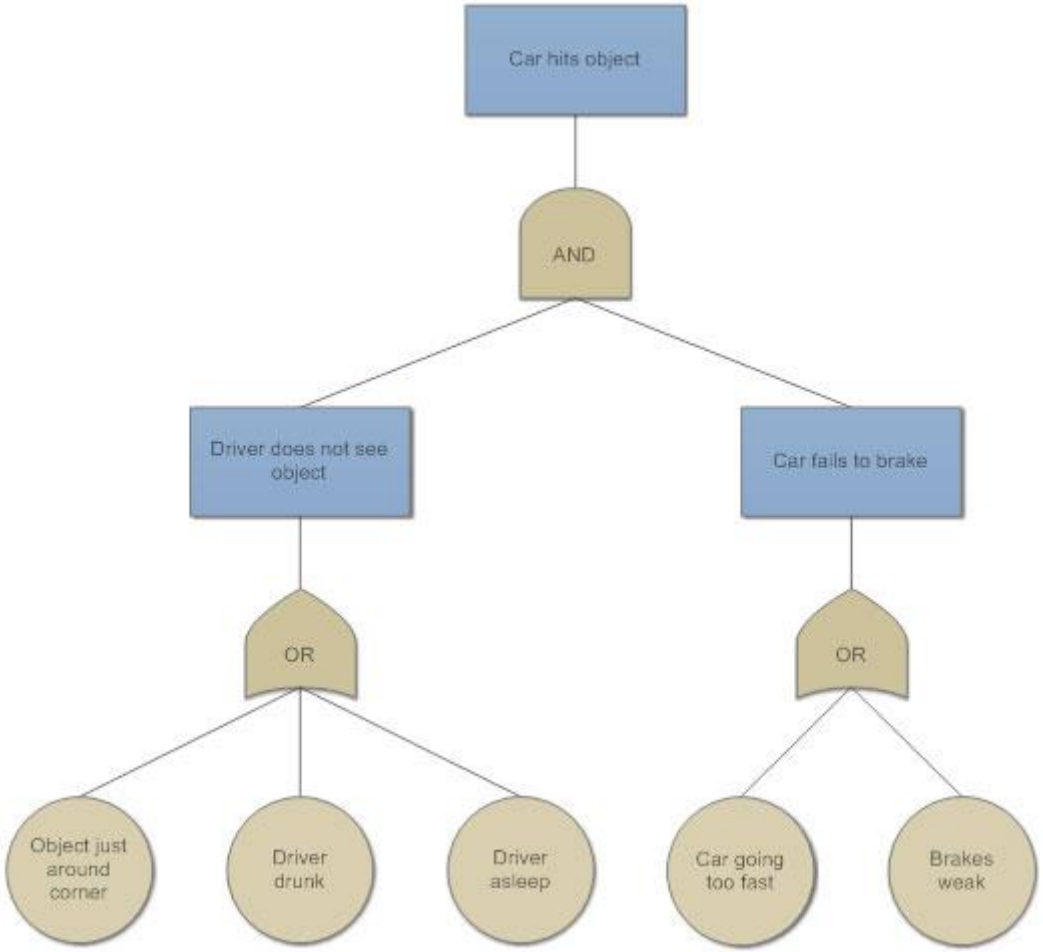
Picking the Top-Level Event

- This is the hardest part of FTA
  - Determines what you analyze in ways that may be subtle
- To analyze . . .
  - Safety
    - Top Level Events are all the ways cause harm
  - Remediation goal
    - Top Level Events are the in-scope documents or processes; e.g., hazardous situations
  - Connections between Risks and Risk Control measures
    - Top Level Events are patient Risks (per ISO/TR 24971:2013, section 6.2 c)
  - Success Planning
    - Top Level Event is a product launch
  - Etc.

How do you build a Fault Tree?

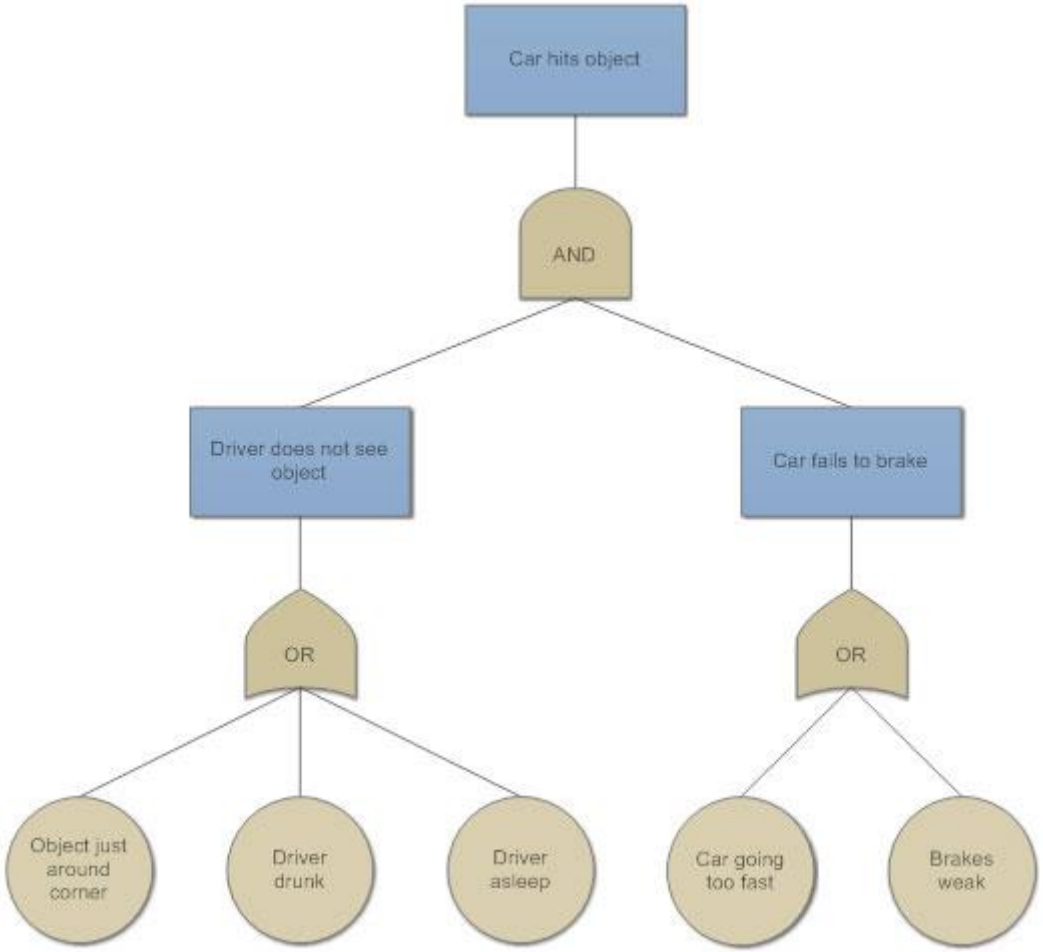
IEC 61025, section 7.4.2:

- The "immediate cause" concept requires that the analyst determine the immediate necessary and sufficient causes for the occurrence of the top event.
- Strict adherence to the concept of "immediate cause" is necessary to ensure that fault modes are not omitted by reason of the assumption that such modes have been included previously.
- IEC 61025, section 6.3:
  Events arising from all causes shall be . . . included in the fault tree.



How do you build a Fault Tree (Cont.)?

- Initial draft goes faster than people expect
  - Basically, a brainstorming session – creativity is key
  - Going from one level to the next becomes fairly quick / routine
- Initial draft needs review by cross-functional SMEs
  - No one person will create a complete FTA
  - Deep specialty knowledge helps most



How do you build a Fault Tree (Cont.)?

- ‘Tricks’ to develop complete FTAs
  - The goal is to establish the necessary and sufficient conditions for each immediate cause
    - If we say that "x is a necessary condition for y," then we mean that if we don't have x, then we won't have y. In other words, without x, you won't have y.
    - If we say that "x is a sufficient condition for y," then we mean that if we have x, we know that y must follow. In other words, x guarantees y.
  - To capture ‘all causes’, examine each event all points in time
    - Installation, Use, Removal, Misuse, Service, Etc.
  - Make sure the causal link from one level to the next is intuitively clear
    - Self-documents causal links that are far from obvious after 3 or 5 levels
  - IEC 61025, section 7.4.2:
  - The concept of "basic units" can be used to save the analyst the effort of developing fault tree diagrams which do not yield new or useful information. A basic unit is treated as if it were a single unit or component or dealt with separately.

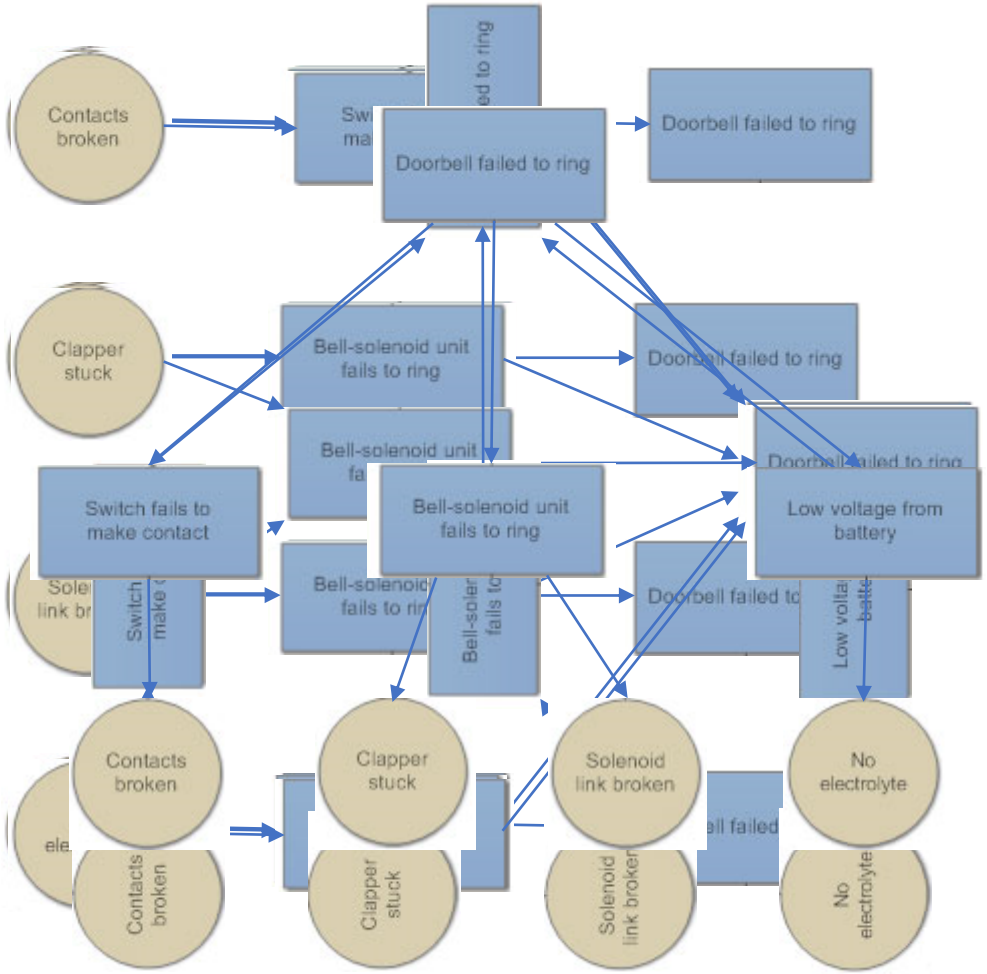
Comparing FMEAs and FTAs

- FMECAs (Failure Mode Effects and Criticality Analysis) started before FTAs
  - Originally developed in 1949 to study munitions failures & was very effective.
  - Later simplified to FMEA (1970s) by removing probability statistics
- Critical problem with FMEAs:
  If you are analyzing anything less than every cause of every element in the system, you never know when you are done.
- In contrast, with an FTA, you are done when you've identified all of the causes of all of the top-level events.

What is the relationship between FMEAs and FTAs?

Rearranged FMEAs for a Doorbell

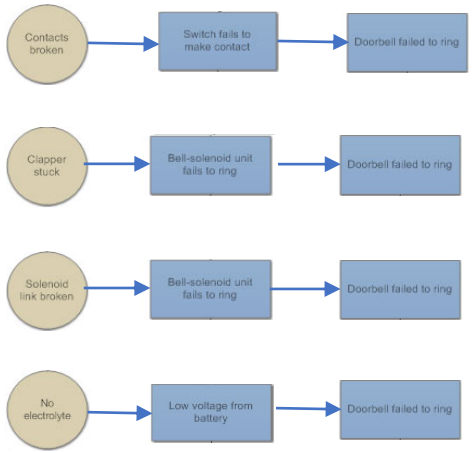
Created FMEAs for a Doorbell

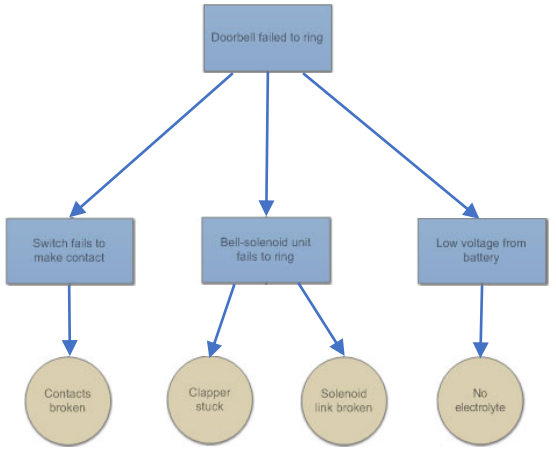


Therefore, an FTA and FMEA hold the same information

So, what else is the same, and What is different between them?

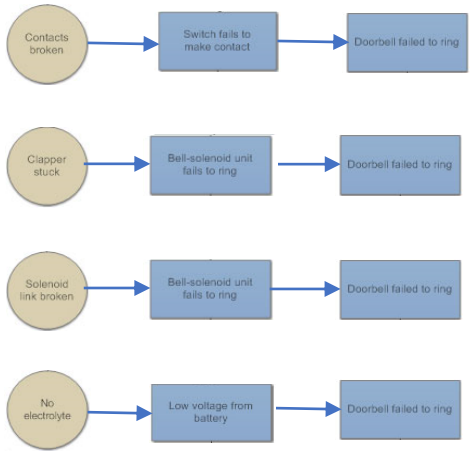
Created an FTA from FMEAs

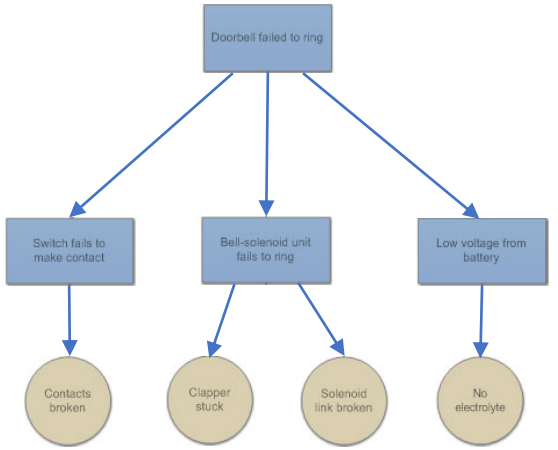




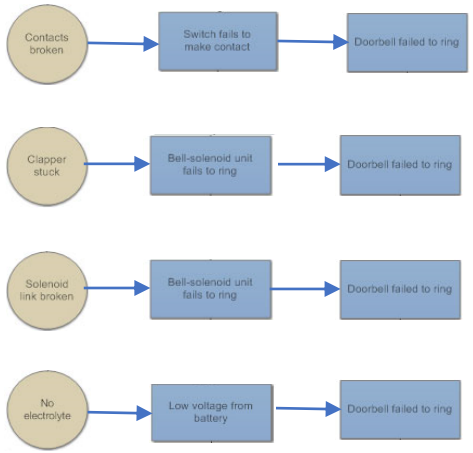
- Every causal thread in a FMEA has a causal thread in a FTA, and visa versa.

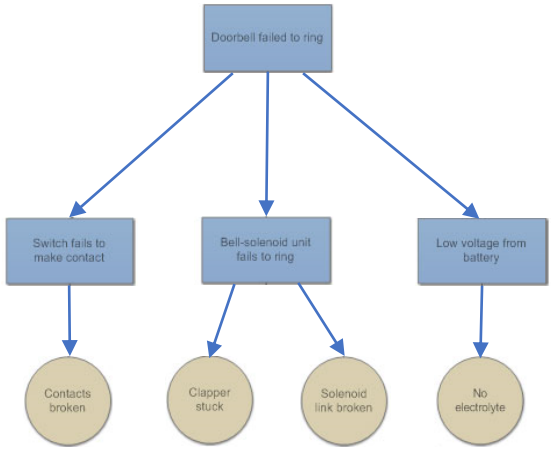
- Each FMEA is an independent thread, while
  an FTA combines common elements to merge portions of threads
  - Combining elements creates many FTAs within one FTA





- FMEAs answer the question:
  If something fails, then what happens?
  - Bottom-up
- FTAs answer the questions:
  What are all of the things that could cause something to fail?
  - Top-Down
- Which question are you asked more often?
  - FTAs answer the core question in root cause investigations





- Consider a pFMEA:
  - How deeply into a design will an FMEA go?
    - To determine production failure modes, the FMEA author has a tradeoff:
      - Start high-enough in the design that they can intuitively see the FMES will connect to a production failure, or
      - Start low-enough in the design that many FMEAs won't result in a production failure.
    - The first approach doesn't get down to component features and production parameters
    - The second approach is so inefficient that people avoid it.
  - An FTA analyzes both the entire design and production, and digs down as wanted
    - No tradeoff – you get both a deep dive and efficient work

Consider Safety Analysis

- We need to analyze all of the ways to cause harm.
  - For a medical application: FDA recommends using a FTA, where the top-level events are the ways that the product can harm the patient
    - This could be expanded to include harm to users
    - The list is shorter than you might expect
      - Many harms are basic physiology and not directly connected with the product
      - Pain, access site reaction or erosion, hypertension, etc.
  - Create one FTA for each harm
    - The FTA will, in one tree, capture all of the causes of this harm
      - Generally between 5 and 30 Fault Trees in the FTA
    - The FTAs will identify critical-to-safety features and parameters from design, production, use, service

Consider Safety Analysis (Cont.)

- Repetition occurs both between, and within, Fault Trees
  - This repetition means individual Fault Trees can be created more quickly than it might seem
  - The concept of "basic units" can be used to identify, and represent, repeated groups of causes. (IEC 61025, section 7.4.2)
- Collect the bottom-level events (causes) from all of the Fault Trees
  - Eliminate duplicates
  - The result is a **list of every safety-critical specification in the product**
    - This list will **contain between 5% and 10%** of the product's specifications
    - Traces to Design (V&V), Production (pFMEA), User (IFU), Service Schedule and Manual
  - Starting FMEAs 'too high' makes virtually all specifications safety-critical

Consider Incoming Inspection

- An FTA on Safety Analysis will identify all ‘safety-critical’ features
  - Use the fact that this FTA will identify between 5% and 10% of component features as ‘safety critical
  - Identifying ‘safety critical’ component features can justify an inspection plan that looks very carefully at a few safety-critical features and much less carefully for most non-safety-critical features.
  - Result:
    A significant reduction in inspection cost and time, with no reduction in safety

Consider Essential Performance

- IEC 60601 – Essential performance is defined as “performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the MANUFACTURER results in an unacceptable risk”.
  - ‘Essential performance’ is most easily understood by considering whether something’s absence or degradation would result in an unacceptable RISK.
- We already reviewed how to identify safety-critical component features / process parameters
- We now propose how to establish Essential Performance

Consider Essential Performance (Cont.)

- Per ISO/TR 24971:2013, section 6.2 c, an FTA of risks will analyze the connections between Risks and Risk Control measures.
- Per ISO 60601, ‘Essential performance’ is most easily understood by considering whether something’s absence or degradation would result in an unacceptable RISK.
- Proposal:
  - ‘Essential performance’ requirements are the component features or process parameters that prevent an unacceptable risk.
  - ‘Essential Design Outputs’ are design outputs that trace to ‘Essential performance’ requirements.

Consider Essential Performance (Cont.)

- What about Safety? Consider an autoinjector (think ‘epi pen’)
  - Life Saving Treatment – Cap Removal Force IS an EPR
  - Non-Life Saving Treatment – Cap Removal Force is NOT an EPR
- Additional FDA examples of Essential Performance Requirement for a Life-Saving Autoinjector
  - Activation Force
  - Needle insertion depth
  - Delivered Volume
  - Injection Time

Questions?