Fault Tree Analysis

Clint Guymon, PhD PE

Brigham Young University

1st Jan, 2025

created in Curvenote

Keywords Spiritual Safety, Process Safety, Chemical Engineering, Risk Assessment

Learning Outcomes

- Construct a Fault Tree Analysis (FTA) using deductive logic to map lower-level failures to a top-level hazardous event.
- Use Boolean logic gates (AND, OR) to combine contributing factors like equipment failure and human error.
- Identify steps to determine the combination of failures required to cause a system failure.

Reading

- Foundations of Spiritual and Physical Safety: with Chemical Processes; Chapter 5, Sections 2.2
- Fault Tree Analysis: Fault tree analysis

Fault tree analysis (FTA) is a top-down, deductive failure analysis in which an undesired state of a system is analyzed using boolean logic to combine a series of lower-level events. This analysis method is used to understand how systems can fail, to identify the best ways to reduce risk, and to estimate event rates of a safety accident or a particular system level (functional) failure.

1 Fault Tree Analysis (FTA): Commuting to Work or School

1.1 Procedure

Commute to work or school avoiding injury from a traffic accident or other hazards. Some events during that commute could be:

- crossing the street on foot
- driving a car through a neighborhood
- driving a car through a busy intersection

- driving a car on a two-lane highway
- driving a car on a freeway
- driving a car through a high-pedestrian area

2 Fault Tree Analysis (FTA): Heated Batch Reactor

2.1 Procedure

A batch reactor is used to complete a reaction needed for the benefit of others. The reactor process has the following processing steps:

1. The reactor is filled with the raw material, a somewhat toxic material.
2. The reactor is heated to the desired temperature (100 F).
3. The reactor is pressurized to the desired pressure (20 psig).
4. Reactant B is slowly added to the reactor. An exothermic reaction occurs and the jacket must begin to cool the reactor to maintain the desired temperature.
5. The reaction proceeds at a given reaction rate at that temperature and pressure until all of the reactant B has been added.
6. The reactor is cooled to room temperature and the product is removed.

2.2 Some Hazards

- Product C has a low boiling point and is toxic. If the reactor is not cooled properly, the product will vaporize and escape from the reactor.
- If stirring is not maintained, the reaction will not proceed at the desired rate and the reactor will overheat.
- Reactor is used for multiple products

Figure 3: Image of the batch reactor credit to: https://www.essentialchemicalindustry.org/processes/chemical-reactors.html

3 Fault Tree Analysis (FTA): MTV Flares

A batch mixing process is used to mix the Magnesium, Teflon, and Viton with a solvent to make an aerial flare. The aerial flare can be used as a decoy to distract heat-seeking missiles from hitting an aircraft. Viton, a fluoroelastomer binder, is disolved in a solvent and then carefully mixed with the Magnesium and Teflon powders. The solvent then evaporates and the particles are coated with viton. The mixture can release significant energy and is sensitive to ignition.

The batch mixing process can have the following processing steps:

1. Binder preparation: Viton is dissolved in a solvent to create a binder solution.
2. Powder mixing: Magnesium and Teflon powders are carefully mixed together in a controlled environment to prevent ignition.
3. Binder addition and mixing: The binder solution is slowly added to the powder and the mixture is thoroughly mixed to ensure uniform coating of the powders with the binder.

4. Granulation and Solvent evaporation: The solvent is allowed to evaporate under processing condition, leaving behind the granulated coated powders.
5. Pressing: The granules are pressed into the desired shape for the aerial flare.
6. Machining or Cutting: The pressed material is machined or cut into the final shape of the aerial flare.

4 Fault Tree Analysis (FTA): Seat Belt Pre-tensioner

Seat belt pre-tensioners are devices that automatically tighten the seat belt in the event of a collision, helping to secure the occupant in place and reduce the risk of injury. The pre-tensioner activates before the airbag deploys, ensuring that the occupant is properly restrained during a crash.

The pre-tensioner contains a small reactive charge that ignites when a collision is detected, causing a piston to rapidly pull the seat belt tight. This mechanism helps to minimize the forward movement of the occupant and can significantly reduce the severity of injuries in a crash.

Processing steps for the seat belt pre-tensioner include:

1. Fill the pre-tensioner with the reactive charge.
2. Seal the pre-tensioner to prevent leaks (or contamination).

5 Fault Tree Analysis (FTA): Bhopal Disaster

The Bhopal disaster was a gas leak incident in India, considered one of the world's worst industrial disasters. It occurred on the night of December 2-3, 1984, at the Union Carbide India Limited (UCIL) pesticide plant in Bhopal, Madhya Pradesh. The disaster resulted in thousands of deaths and injuries due to the release of methyl isocyanate (MIC) gas.

The incident was caused by a combination of factors, including poor maintenance, inadequate safety measures, and human error. The gas leak occurred when water entered a storage tank containing MIC, leading to a chemical reaction that produced a large amount of toxic gas.

You can read more about the Bhopal disaster here: Bhopal disaster and elsewhere.

6 Spiritual FTA

7 Combination of FTA and FMEA:

An accident investigation prior to the accident

Example start on an FTA: (lower left is 'Blades fall off')

Example start of the FMEA/ Hazards Analysis

Link to a template for HAZOP documentation: https://github.com/clint-bg/safetyinjc/blob/main/exports/FMEA Template.docx

Action Items

1. Draw a Fault Tree Diagram for the production of polyethylene. Most safety concerns are around the plug flow reactor with a highly exothermic reaction occurring. A compressor is used to pressurize the ethylene feed to near 1500 bar. A cooling jacket surrounds the plug flow reactor where the temperature is controlled to near 70C. A separator is then used to collect the polyehtylene solids and the unreacted ethylene is recycled.

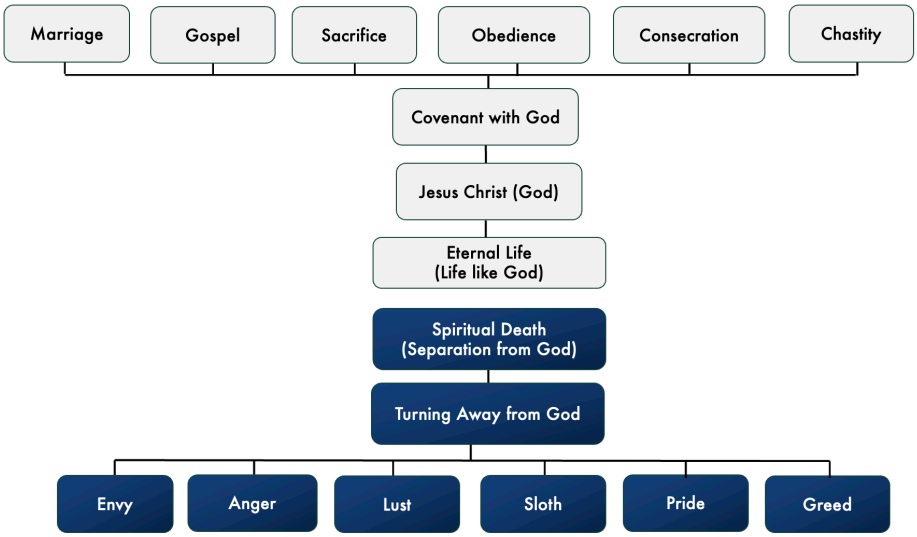

Figure 4: Spiritual FTA Example

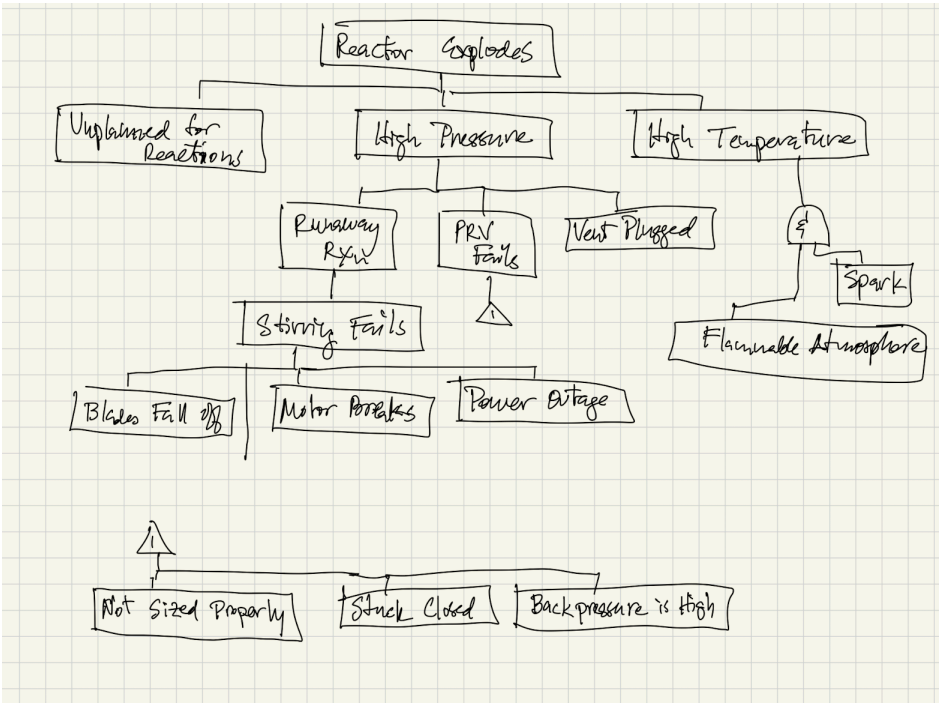

Figure 5: Example Fault Tree Analysis

BYU TIPICE

Job Hazards Analysis (JHA)

Title:	Document No.:	Page:
Operator/ Test Individual:	Rev:	Date:

BYU CH EN Job Hazards Analysis						
Task Description	**Hazard Type**	**Hazard Description**	**Consequence**	**Safeguards**	**Rank**	**Recommendations**
Reactor Operation - Stirring	Electrical Failure	Controller Fails from Power Outage	Stirring ceases resulting in a runaway reaction, high pressure, and potential violent reactor explosion	Battery Powered alarm present to indicate power failure Backup power generator present	2D	
Reactor Operation - Stirring	Component Failure	Motor Fails	Stirring ceases resulting in a runaway reaction, high pressure, and potential violent reactor explosion	Alarm present on motor indicating presence of stirring Emergency venting of reactor contents possible	2D	

Figure 6: FMEA Example

2. Identify a "Top Level Event" for a commute to school and deduce at least three sub-events that could lead to that outcome.

3. Comment on the both the success and failure portions of the Fault tree for spiritual scenarios FIgure V.10(Guymon, 2025) page (95). What covenants have you made or could you make with God to help you succeed and draw closer to God?

References

C. Guymon. *Foundations of Spiritual and Physical Safety: with Chemical Processes*. 2025.