Traditional Safety Analysis

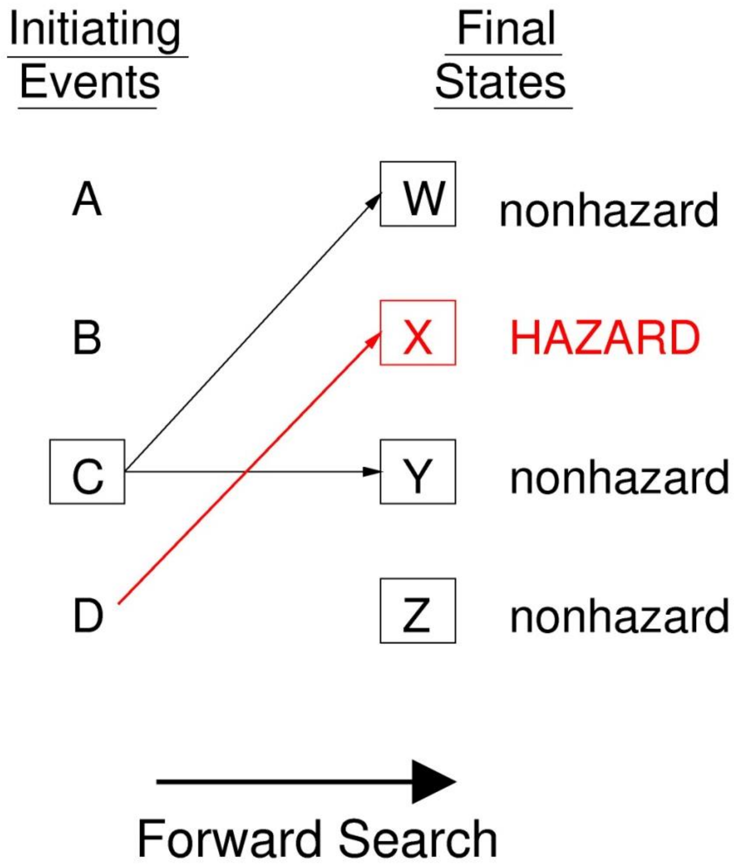
Qualitative Methods

Agenda

- Today: Qualitative methods
  - FMEA
  - FTA
  - HAZOP
  - Limitations
- Thursday: Quantitative methods
  - FMECA
  - FTA
  - PRA?
  - Limitations

FMEA: Failure Modes and Effects Analysis

- 1949: MIL-P-1629
- Forward search technique
  - *Initiating event*: component failure
  - *Goal*: identify effect of each failure

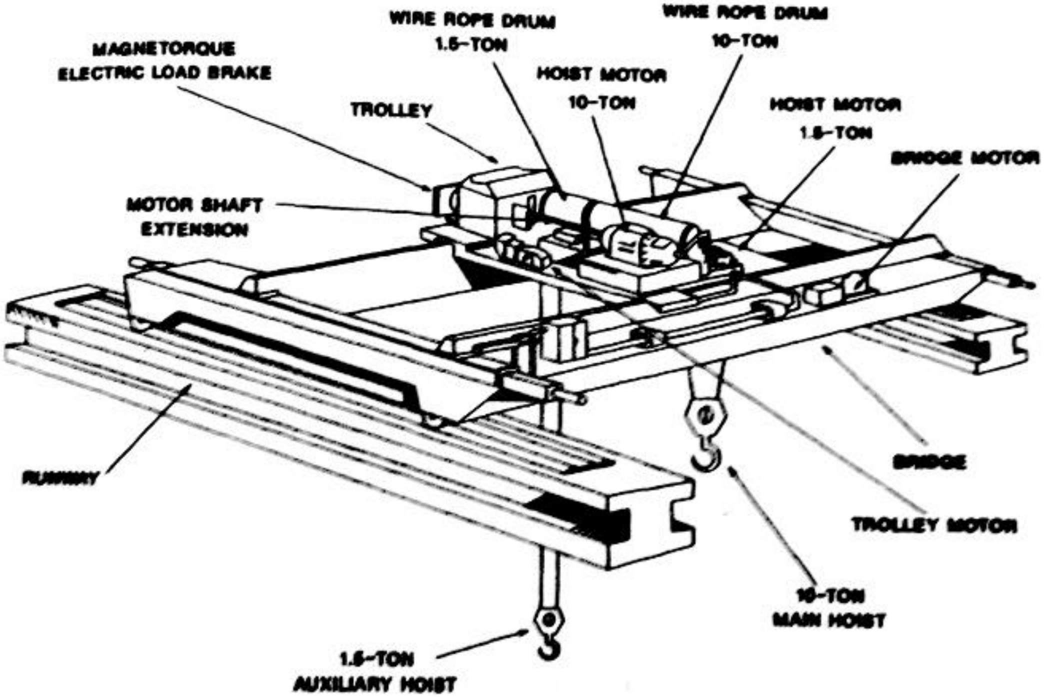


General FMEA Process

1. Identify individual components
2. Identify failure modes
3. Identify failure mechanisms (causes)
4. Identify failure effects

FMEA worksheet

Example: Bridge crane system



Failure Mode and Effect Analysis

Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:_________

Component Name	Failure Modes	Failure Mechanisms	Failure effects (local)	Failure effects (system)
Main hoist motor	Inoperative, does not move	Defective bearings Loss of power Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.

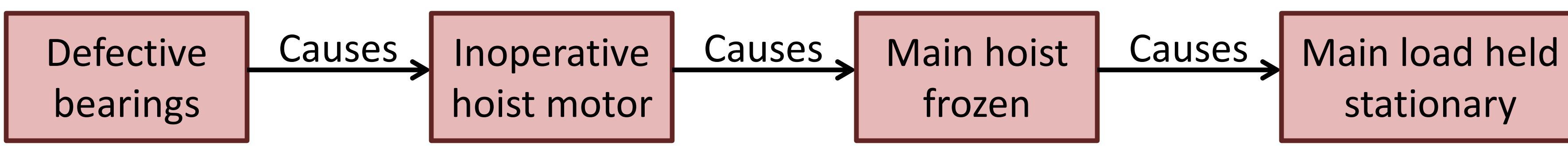
*FMEA example adapted from (Vincoli, 2006)

FMEA uses an accident model

FMEA method:

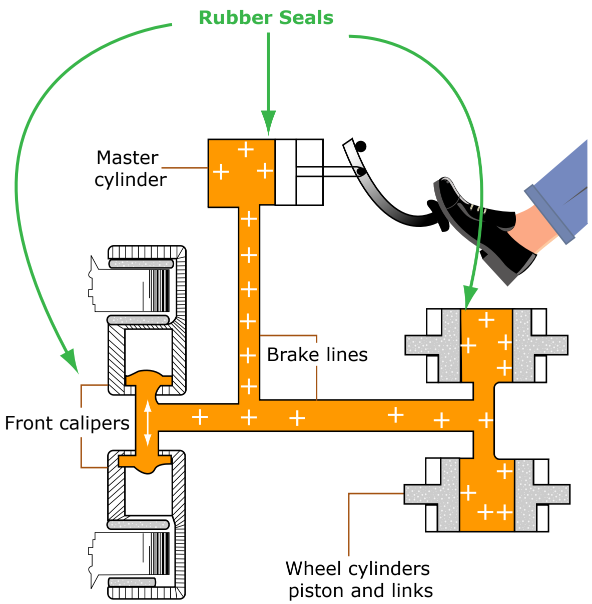
Failure Mode and Effect Analysis				
Program:__________ Engineer:__________		System:__________ Date:____________		Facility:_________ Sheet:__________
Component Name	**Failure Modes**	**Failure Mechanisms**	**Failure effects (local)**	**Failure effects (system)**
Main Hoist Motor	Inoperative, does not move	Defective bearings Loss of power Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.

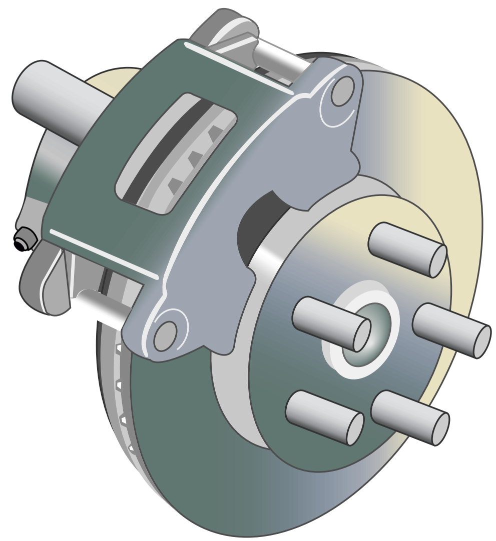
Accident model: Chain-of-events

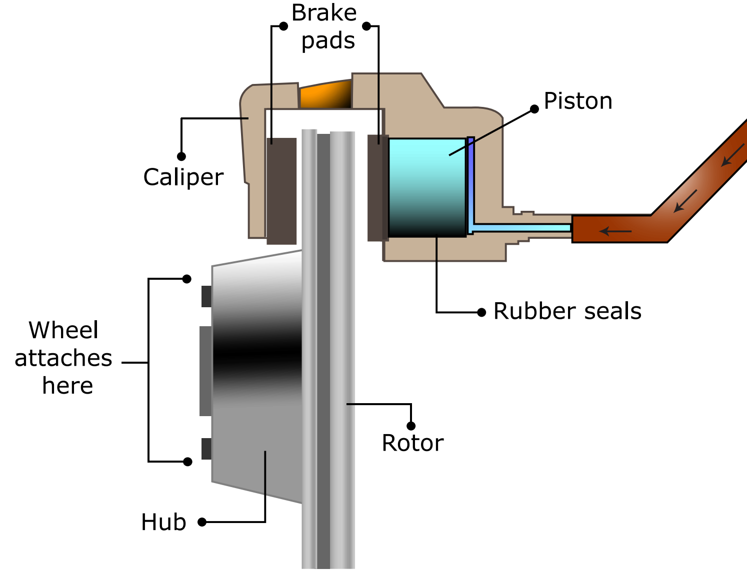


*FMEA example adapted from (Vincoli, 2006)

FMEA Exercise
Automotive brakes







Images by MIT OpenCourseWare.

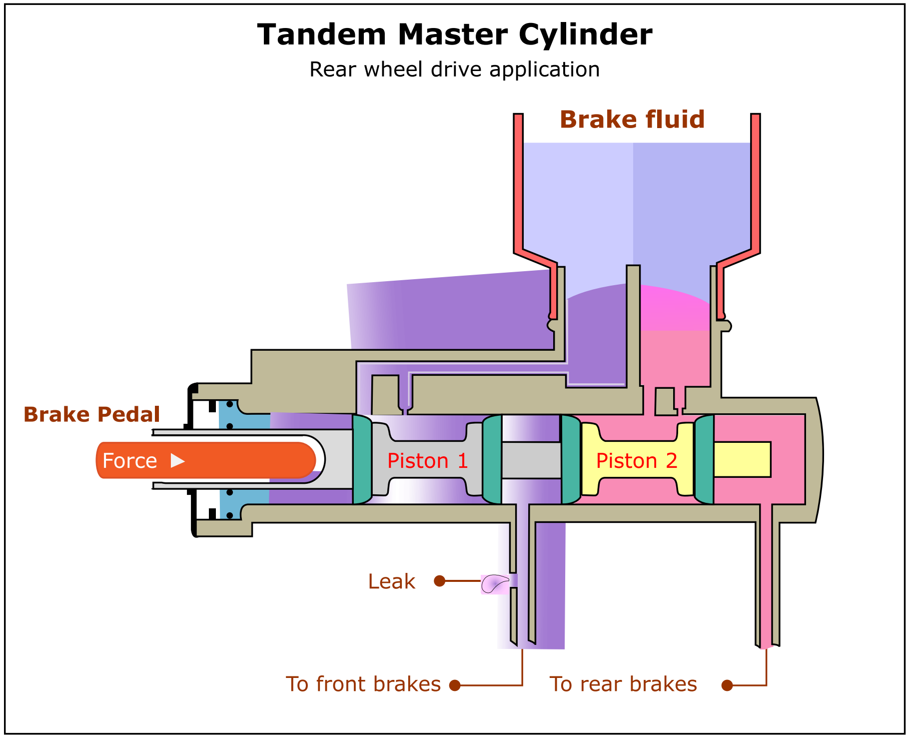
System components

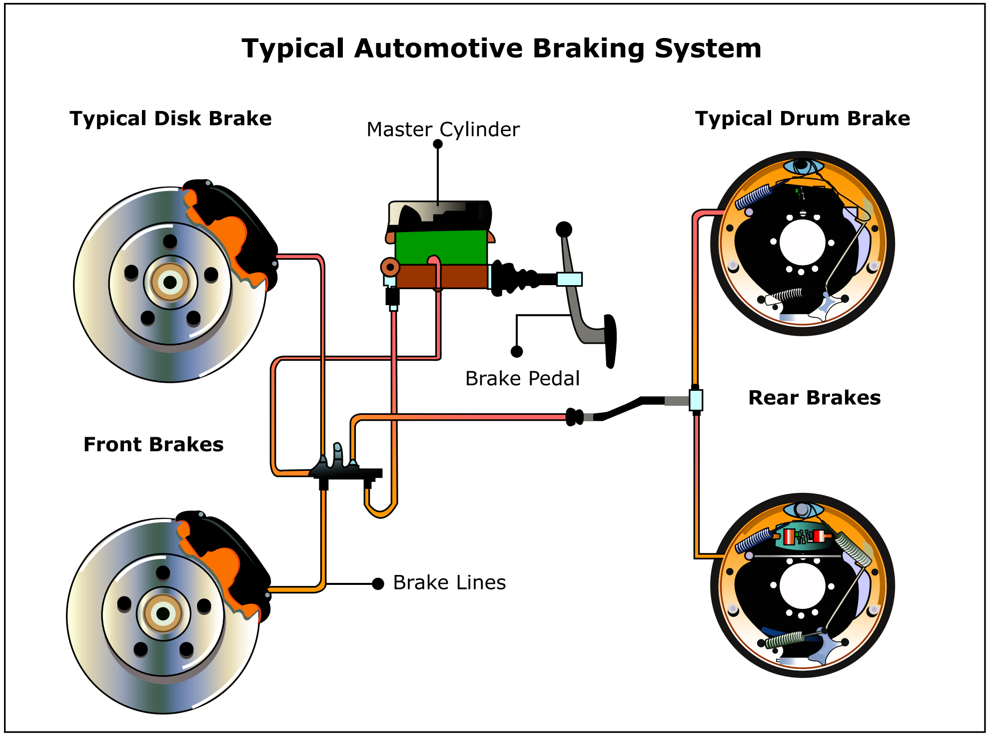
- Brake pedal
- Brake lines
- Rubber seals
- Master cylinder
- Brake pads

FMEA worksheet columns

- Component
- Failure mode
- Failure mechanism
- Failure effect (local)
- Failure effect (system)

Actual automotive brakes





Images by MIT OpenCourseWare.

- FMEA heavily used in mechanical engineering
- Tends to promote redundancy
- Useful for physical/mechanical systems to identify single points of failure

A real accident: Toyota's unintended acceleration

- **2004-2009**
  - 102 incidents of stuck accelerators
  - Speeds exceed 100 mph despite stomping on the brake
  - 30 crashes
  - 20 injuries
- **2009, Aug**:
  - Car accelerates to 120 mph
  - Passenger calls 911, reports stuck accelerator
  - Some witnesses report red glow / fire behind wheels
  - Car crashes killing 4 people
- **2010, Jul:**
  - Investigated over 2,000 cases of unintended acceleration

Captured by FMEA?

FMEA Limitations

- Component failure accidents only
  - Design issues? Requirements issues?
- Single component failures only
  - Multiple failure combinations not considered
- Failure modes must already be known
  - Best for standard parts with few and well-known failure modes
- Requires detailed system design
  - Limits how early analysis can be applied
- Works best on hardware/mechanical components
  - **Human** operators? (driver?)
  - **Software** doesn't fail
  - Organizational factors (management pressure? culture?)
- Inefficient, analyzes non-safety-critical failures
  - Can result in 1,000s of pages of worksheets
- Reliability vs. safety
  - (next slide)

Safety vs. Reliability

- Common assumption:

  Safety = reliability

- How to improve safety?
  - Make everything more reliable!
- Making car brakes safe
  - Make every component reliable
  - Include redundant components

Is this a good assumption?

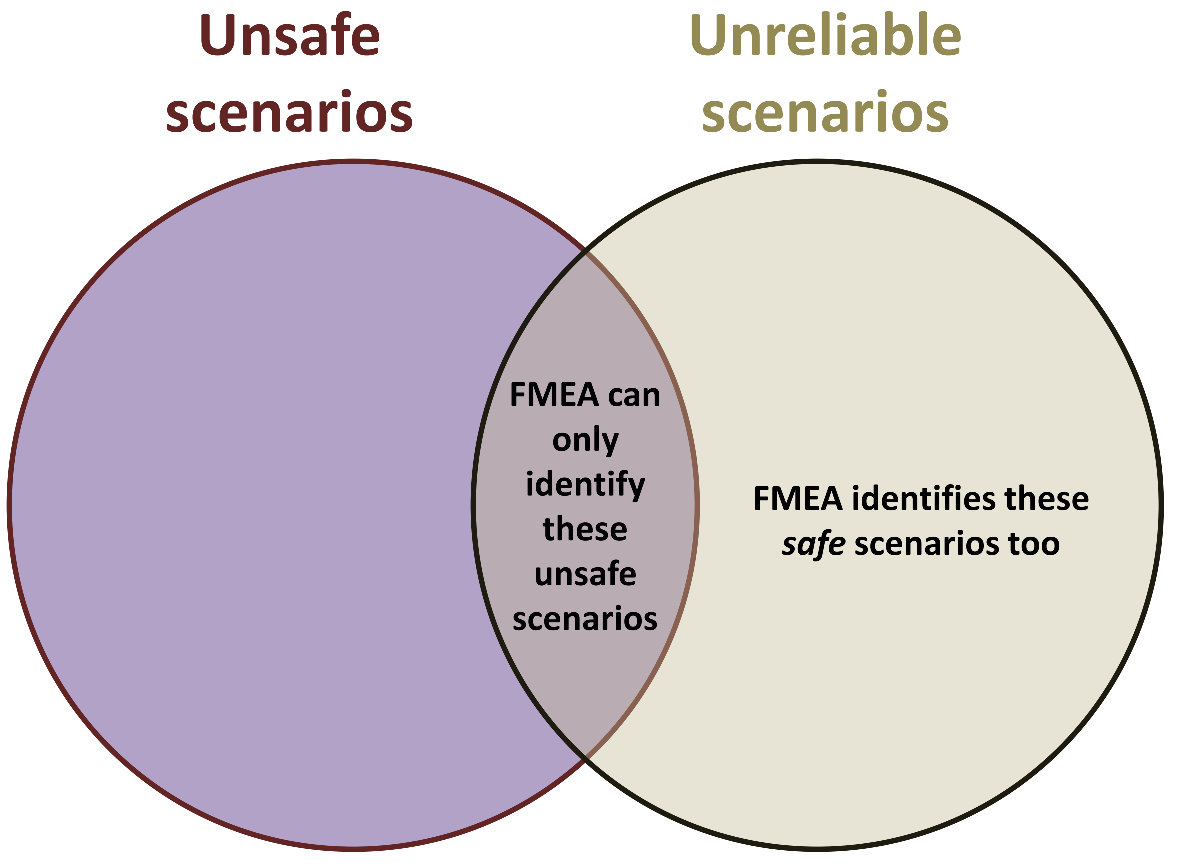
*Image from midas.com

Safety vs. Reliability

- Safe ≠ Reliable
- Safety often means making sure X never happens
- Reliability usually means making sure Y always happens

	Safe	**Unsafe**
Reliable	•Typical flight	•Aircraft reliably runs out of fuel? •A shuttle (inadvertently) designed to hit ISS? •A nail gun? Stapler?
Unreliable	•Aircraft engine won't start on ground? •Automotive "limp" mode? •Missile won't fire?	•Aircraft engine fails in flight

Safety vs. Reliability

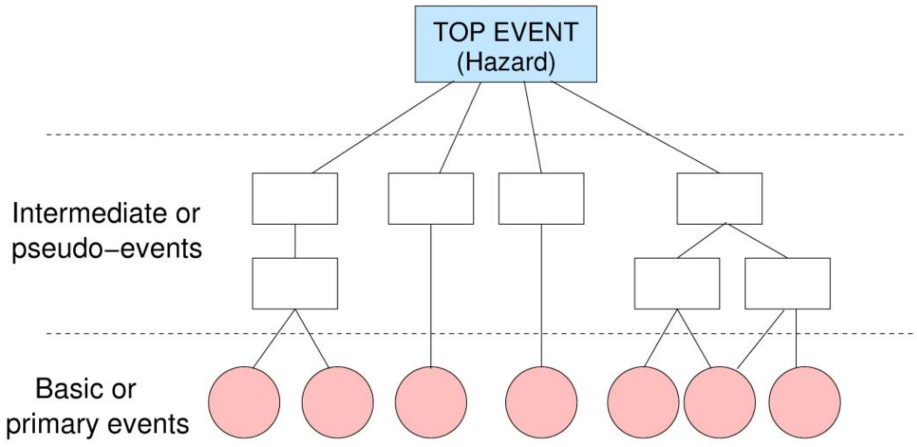


- FMEA is a *reliability* technique
  - Explains the inefficiency; FMEA analyzes non-safety-related failures
- FMEA sometimes used in safety analyses because it establishes the end effects of failures

FTA
Fault Tree Analysis

FTA: Fault Tree Analysis

- 1961: Bell labs analysis of Minuteman missile system
- Today one of the most popular hazard analysis techniques
- Top-down search method
  - Top event: undesirable event
  - Goal is to identify causes of hazardous event



FTA Process

1. Definitions
   – Define top event
   – Define initial state/conditions
2. Fault tree construction
3. Identify *cut-sets* and *minimal cut-sets*

Fault tree examples

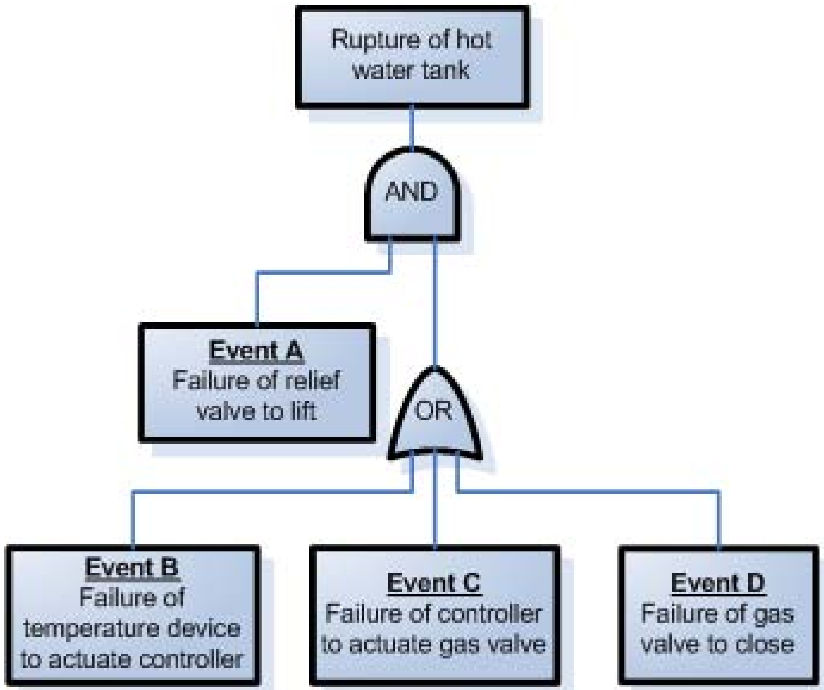


Image: Public Domain. USDOE. SAND2012-4080.

Example from original 1961 Bell Labs study

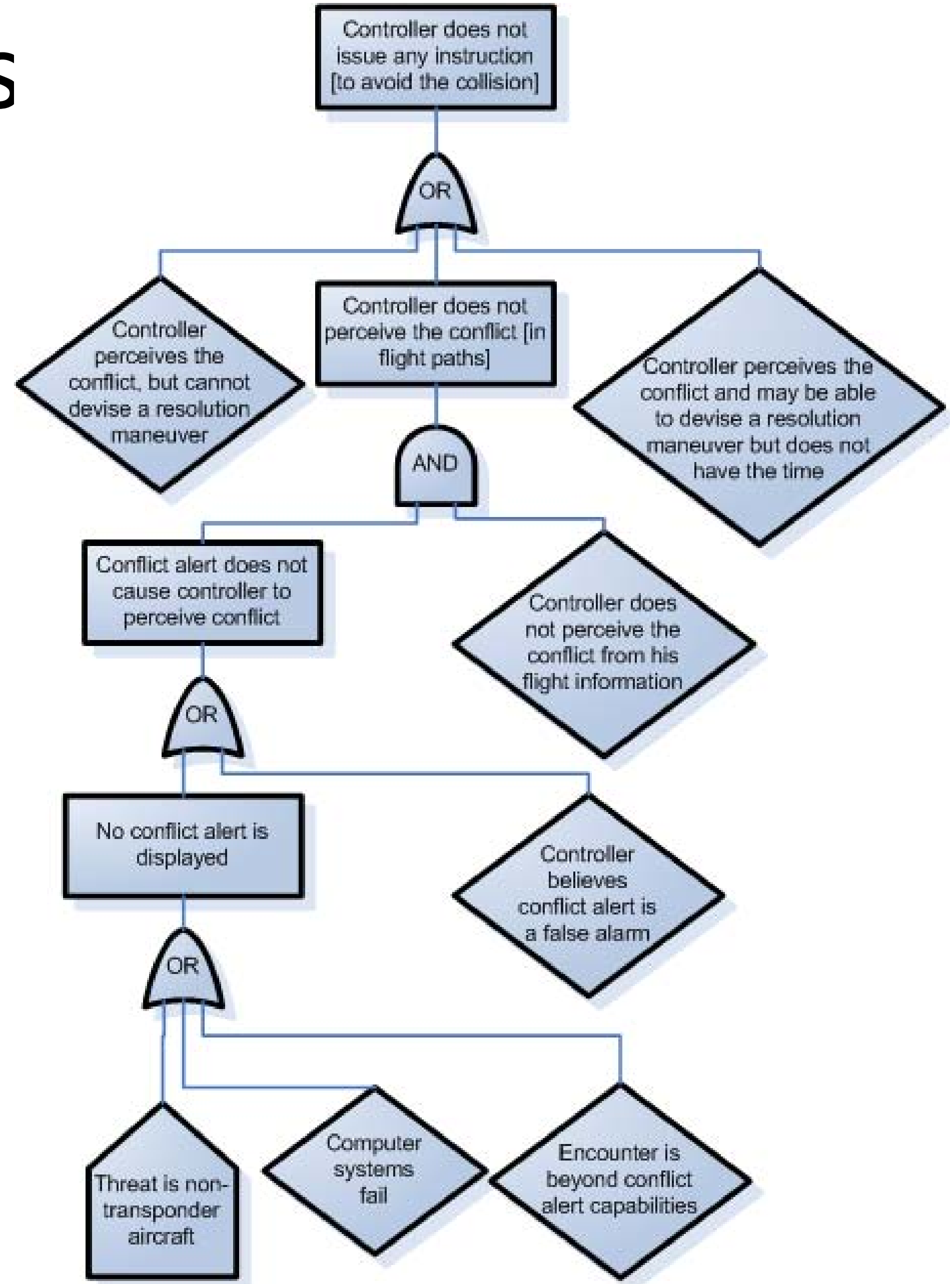
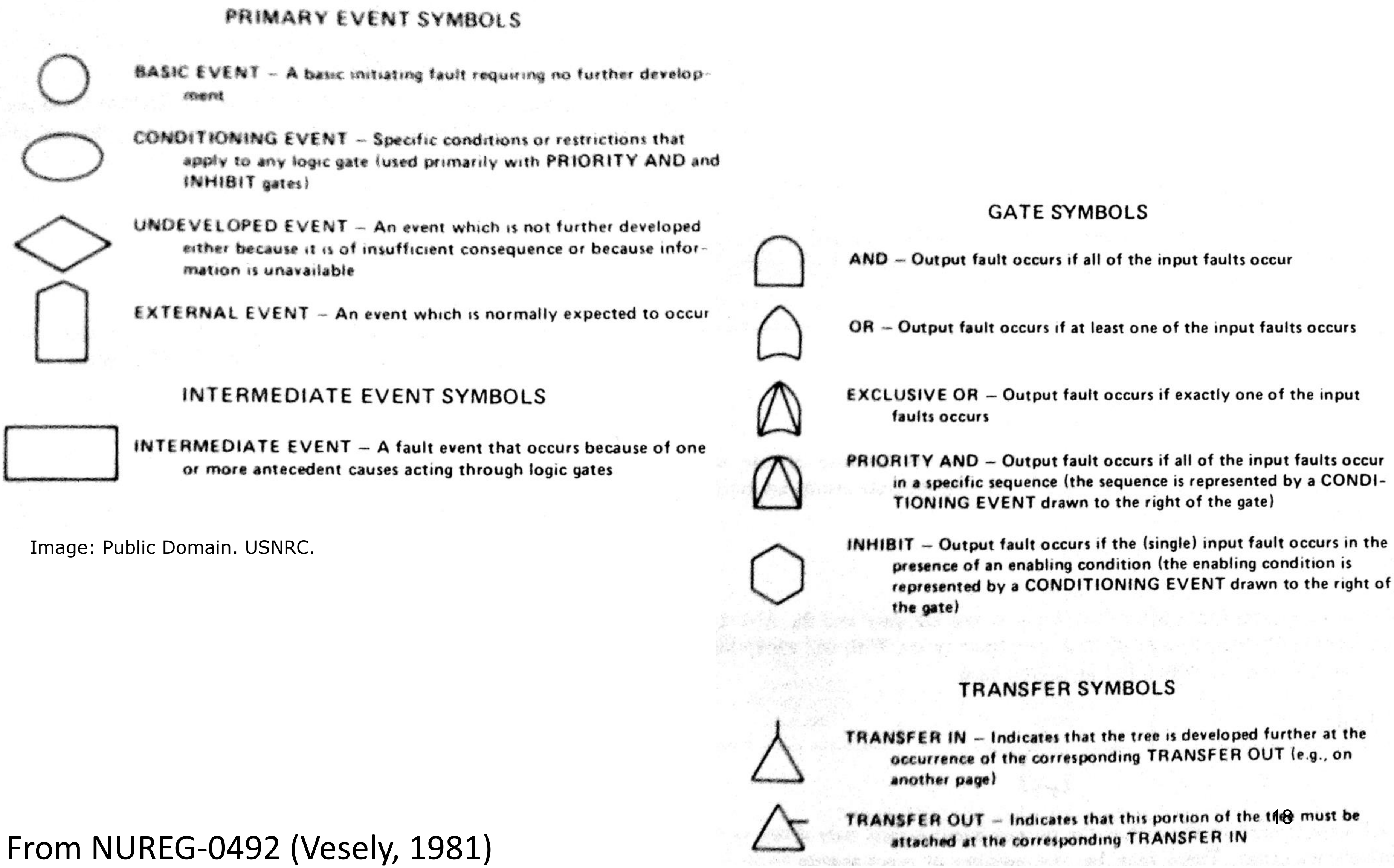


Image: Public Domain. USDOE. SAND2012-4080.

Part of an actual TCAS fault tree (MITRE, 1983)

Fault tree symbols



PRIMARY EVENT SYMBOLS

BASIC EVENT – A basic initiating fault requiring no further development

CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

UNDEVELOPED EVENT – An event which is not further developed either because it is of insufficient consequence or because information is unavailable

EXTERNAL EVENT – An event which is normally expected to occur

INTERMEDIATE EVENT SYMBOLS

INTERMEDIATE EVENT – A fault event that occurs because of one or more antecedent causes acting through logic gates

GATE SYMBOLS

AND – Output fault occurs if all of the input faults occur

OR – Output fault occurs if at least one of the input faults occurs

EXCLUSIVE OR – Output fault occurs if exactly one of the input faults occurs

PRIORITY AND – Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT – Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

TRANSFER SYMBOLS

TRANSFER IN – Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)

TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

From NUREG-0492 (Vesely, 1981)

Fault Tree cut-sets

- *Cut-set*: combination of basic events (leaf nodes) sufficient to cause the top-level event
  - Ex: (A and B and C)
- *Minimum cut-set*: a cut-set that does not contain another cut-set
  - Ex: (A and B)
  - Ex: (A and C)

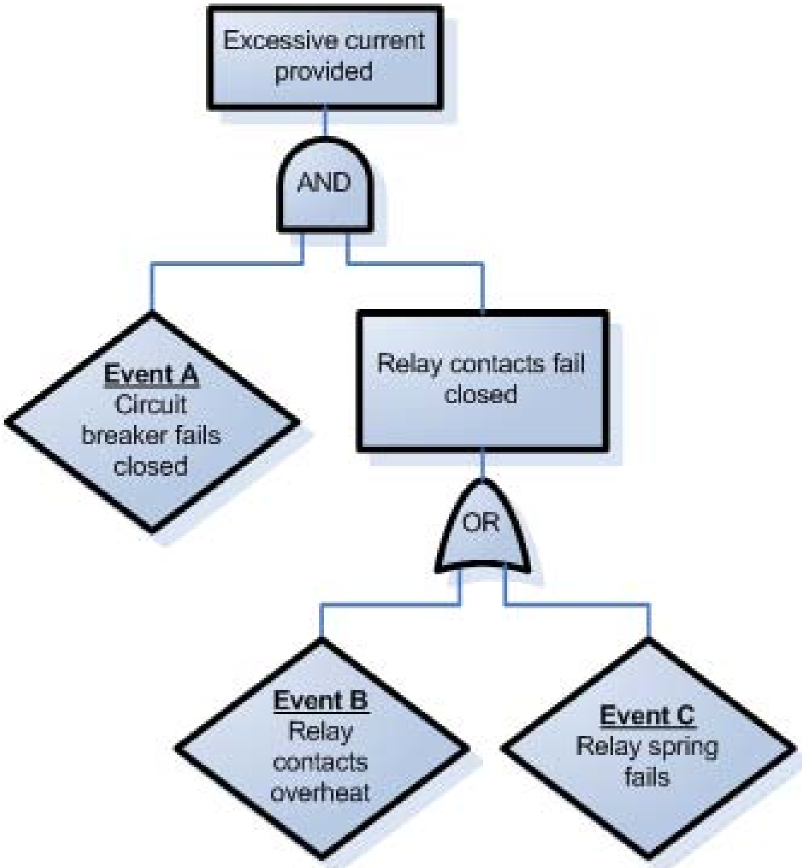


Image: Public Domain. USDOE. SAND2012-4080.

FTA uses an accident model

Fault Tree:

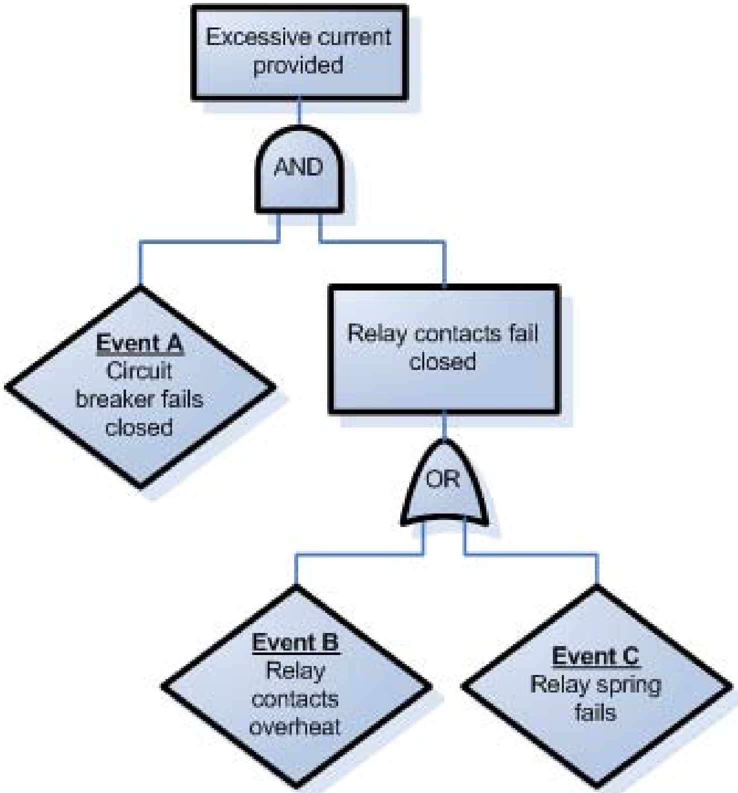


Image: Public Domain. USDOE. SAND2012-4080.

Accident model: Chain-of-failure-events

Fault Tree Exercise

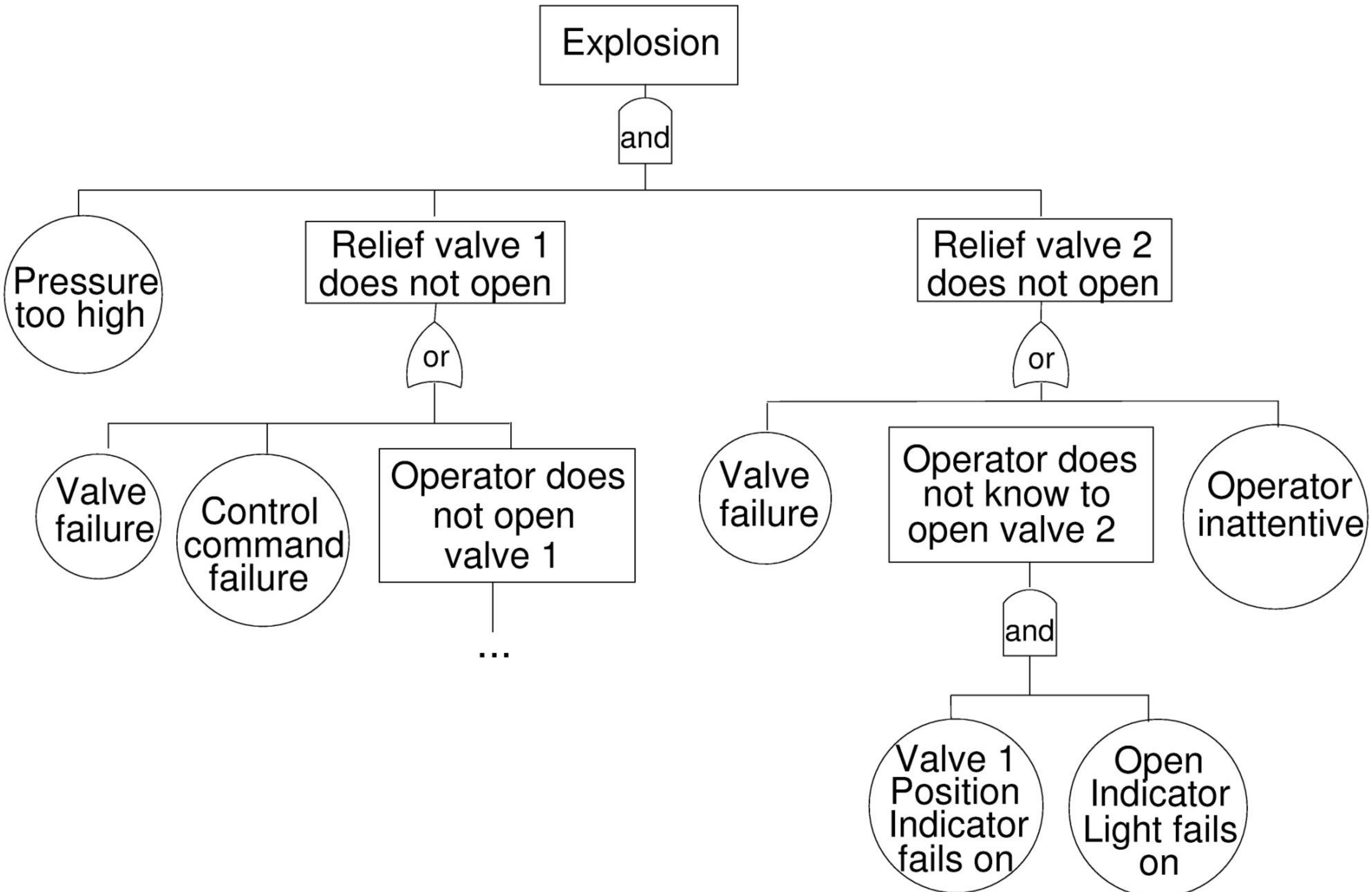
- **Hazard**: Explosion
- **Design**:

System includes a relief valve opened by an operator to protect against over-pressurization. A secondary valve is installed as backup in case the primary valve fails. The operator must know if the primary valve does not open so the backup valve can be activated.

Operator console contains both a primary valve position indicator and a primary valve open indicator light.

Draw a fault tree for this hazard and system design.

Fault Tree Exercise



FTA Strengths

- Captures **combinations** of failures
- More **efficient** than FMEA
  - Analyzes only failures relevant to top-level event
- Provides **graphical format** to help in understanding the system and the analysis
- Analyst has to think about the system in great detail during tree construction
- Finding minimum **cut sets** provides insight into weak points of complex systems

FTA Limitations

- **Independence** between events is often assumed
- **Common-cause failures** not always obvious
- Difficult to capture **non-discrete** events
  – E.g. rate-dependent events, continuous variable changes
- Doesn't easily capture **systemic factors**

FTA Limitations (cont)

- Difficult to capture delays and other **temporal factors**
- **Transitions** between states or operational phases not represented
- Can be **labor intensive**
  - In some cases, over 2,500 pages of fault trees

FTA Limitations (cont)

Inherits general limitations of failure-based methods:

- Component failure accidents only
  - Design issues?
  - Requirements issues?
- Requires detailed system design
- Failure mechanisms must already be known
  - Best for standard parts with few and well-known failure modes
- Works best on hardware/mechanical components
  - **Human** operators?
  - **Software** doesn't fail
  - Organizational factors (management pressure? culture?)

Summary

FMEA and FTA

- Both well-established methods
- Time-tested, work well for the problems they were designed to solve
- Strengths include
  - Ease of use
  - Graphical representation
  - Ability to analyze many failures and failure combinations
  - Application to well-understood mechanical or physical systems
- Limitations include
  - Inability to consider accidents without failures
  - Difficulty incorporating systemic factors like managerial pressures, complex human behavior, and design/requirements flaws
- Other methods may be better suited to deal with the challenges introduced with complex systems