§II - Risk Management

Agenda

- Identification
- Risk Mgmt Techniques
- Types of Risk
- Fault Tree Analysis (FTA)
- FMEA/FMECA
- Common Mode Analysis
- Hazard Analysis
- Risk Matrix
- System Safety
- Mitigation

Definition

ISO Guide 73:2009 defines risk as the effect of uncertainty on objectives.

	Importance	Risk types																						
		Technical			Scheduling				Safety		Financial			Regulatory				Supplier			Materials			Etc.
		A	B	C	A	B	C	D	A	B	A	B	C	A	B	C	D	A	B	C	A	B	C	
Product 1																								
Product 2																								
Product 3																								
Service 1																								
Service 2																								

Example of risk assessment matrix

Risk Identification

Identification of potentially undesirable effects

The challenges include combinations of failures;

- Software – coding functional errors, coding flow errors, etc.
- Hardware – early failures, random failures, wear out, etc.
- Human – cognition errors, observing, interpreting, planning, etc.
- Procedural – calculations, rounding, misuse, etc.
- Logical – correlation, intersubjective agreement, affirming the consequent, etc.
- Etc.

Types of Risk

- **Technical:** technology readiness, change in location/geography, regulation changes, etc.
- **Scheduling:** Are advance planning and provision for contingencies adequate? Will conflicts with schedules of other products impact delivery?
- **Safety:** Will various phases of the life cycle cause health and safety hazards to the user or others? Will proposed changes in processes, materials, and so on, increase health and safety hazards to operators, installers, or others?
- **Financial:** How will changes in exchange rates for international transactions impact the organization? Is the information regarding creditworthiness of customers adequate?
- **Regulatory:** Will domestic/international political trends impact the organization? What expenses or delays will occur to meet proposed regulations?
- **Suppliers:** How would change of status (for example, buyout) of a supplier impact the delivery schedule? Will changes in the transportation infrastructure impact supplies?
- **Materials:** How will changes in cost/availability of key materials impact the product? What effect will supply/demand and international relations have on the product?

Risk Management Techniques

A variety of approaches are used….

Fault Tree Analysis (FTA)

Success Tree Analysis (STA)

Failure Modes Effects Analysis (FMEA)

Failure Modes Effects and Criticality Analysis (FMECA)

Failure Reporting And Corrective Action System (FRACAS)

Preliminary Hazards Analysis (PHA)

Failure Modes Effects and Diagnostic Analysis (FMEDA)

Systems Theoretic Process Analysis (STPA)

FTA
Fault Tree Analysis

Objectives – of the tool

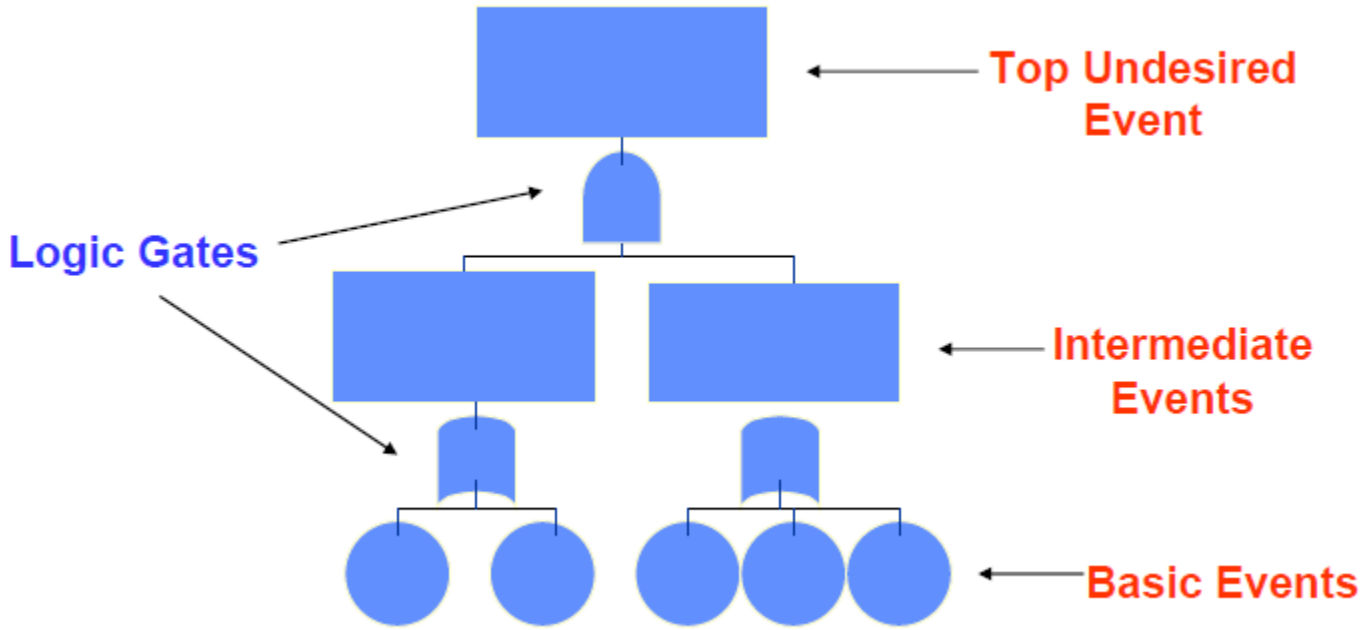
- Deductive ‘top down’ analysis
- Includes inter-relationships
- Provision for probabilities
- Accommodates failure and success
- Relationship to Reliability Block Diagrams

Systematic stepwise (divergent) expansion of potential causal contributors that does not require a dominant failure mode which is a necessary condition for tools like RCA (a convergent problem solving tool)

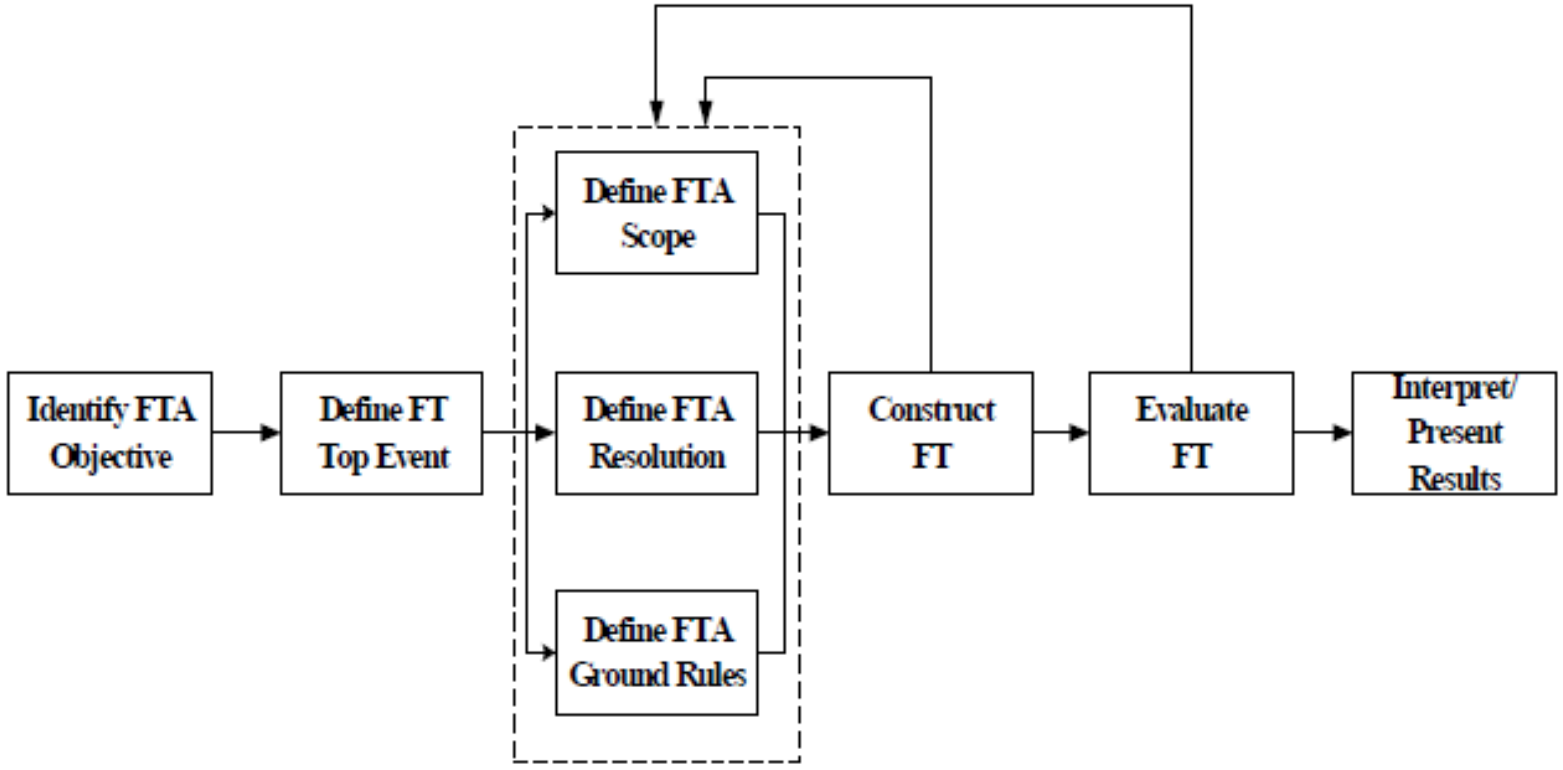
FTA Historical Notes

- FTA as a method to perform risk and reliability assessment surfaced in the early 1960s originated in US aerospace and missile programs.
- It wasn’t until after the Challenger accident in 1986 that NASA began to show greater interest in the probabilistic approach.
- The nuclear industry adopted FTA after the Three Mile Island incident in 1979, and in 1981, the US Nuclear Regulatory Commission (NRC) issued the Fault Tree Handbook, NUREG-0492.

FTA basics


Top Undesired Event
Logic Gates
Intermediate Events
Basic Events

FTA Development Progression



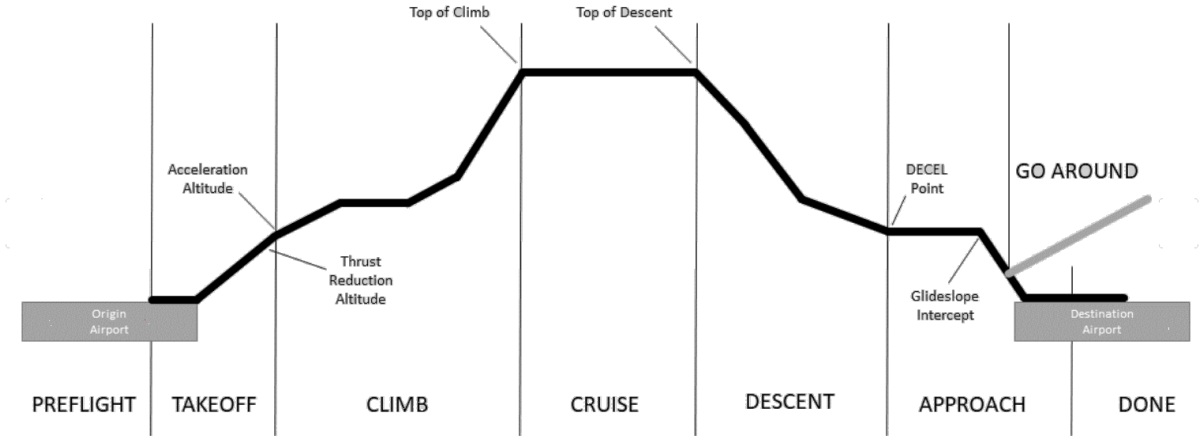
FTA Steps

1. Identify the ***objective*** for the FTA.
2. Define the ***top event*** of the FT.
3. Define the ***scope*** of the FTA.
4. Define the ***resolution*** of the FTA.
5. Define ***ground rules*** for the FTA.
6. ***Construct*** the FT.
7. ***Evaluate*** the FT.
8. ***Interpret*** and present the results.

Steps in Carrying Out a FTA

1. Objective should be phrased in terms of a failure of the system to be analyzed. If this is resolved into a phased mission, i.e. dormant->startup->primary mission leg->shutdown…may require sequential gating or separate FTAs.

2. Establish the top event of the tree (success/failure)



Steps in Carrying Out a FTA

3. Establish the scope of the of the FT. This should include any assumptions (i.e. supplied parts are assumed conformant to design specifications – or not). This may also be a mission leg specific FT, a zonal FT or other.

4. Establish the resolution of the FTA. Define the level of detail to be pursued. Fault trees should be developed to a level of detail where the best failure probability data are available.

Steps in Carrying Out a FTA

5. Define the naming convention to be used, establish the acceptable evidence hierarchy and establish how the information will be tracked and mapped to the FTA.

6. Construction of the FTA, to include any references to original
    RBDs, PFDs, Fish bone diagrams, FMEAs…etc.

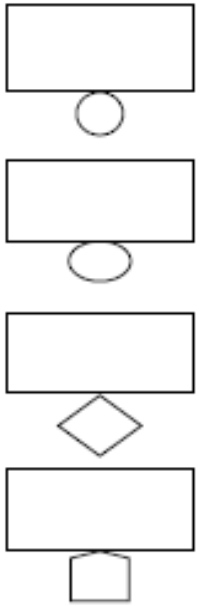
Steps in Carrying Out a FTA

7. Evaluation of the FTA. Cut sets, minimal cut sets, probabilities (with references) and distinctions if mission profile phases are included.

8. Interpretation and recommendations based on the available information. Presentation of the information to decision makers can bias the output.

FTA Symbols

PRIMARY EVENT SYMBOLS



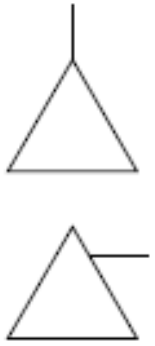
BASIC EVENT - A basic initiating fault requiring no further development

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

HOUSE EVENT - An event which is normally expected to occur

TRANSFER SYMBOLS



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

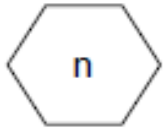
TRANSFER OUT - Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

FTA Symbols

GATE SYMBOLS

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

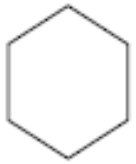
OR - Output fault occurs if a least one of the input faults occurs



COMBINATION - Output fault occurs if n of the input faults occur

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

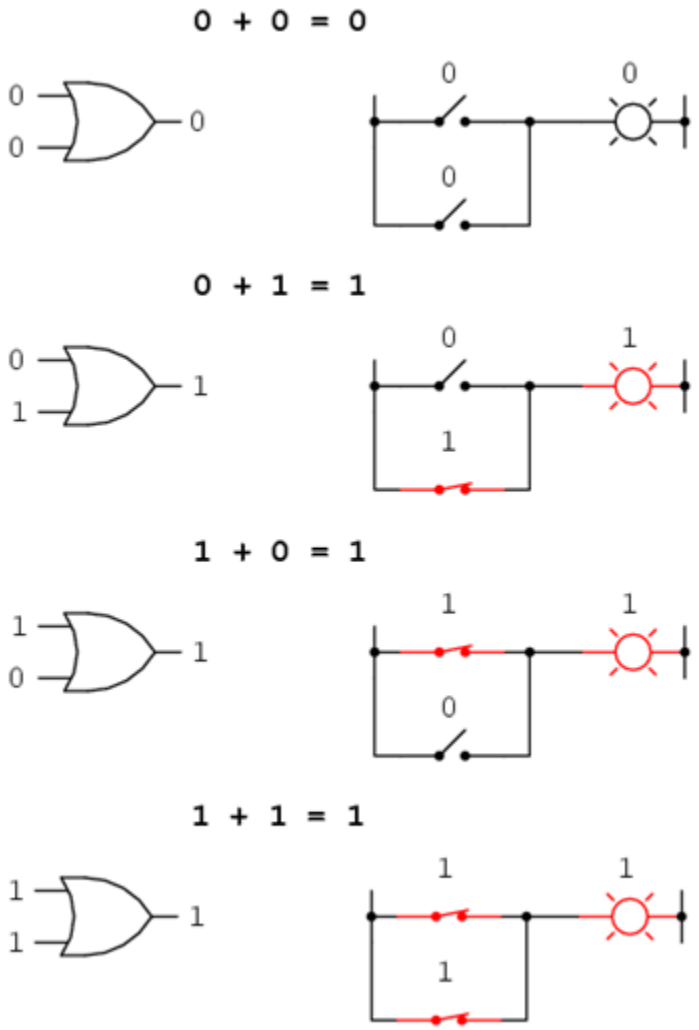
PRIORITY AND - Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

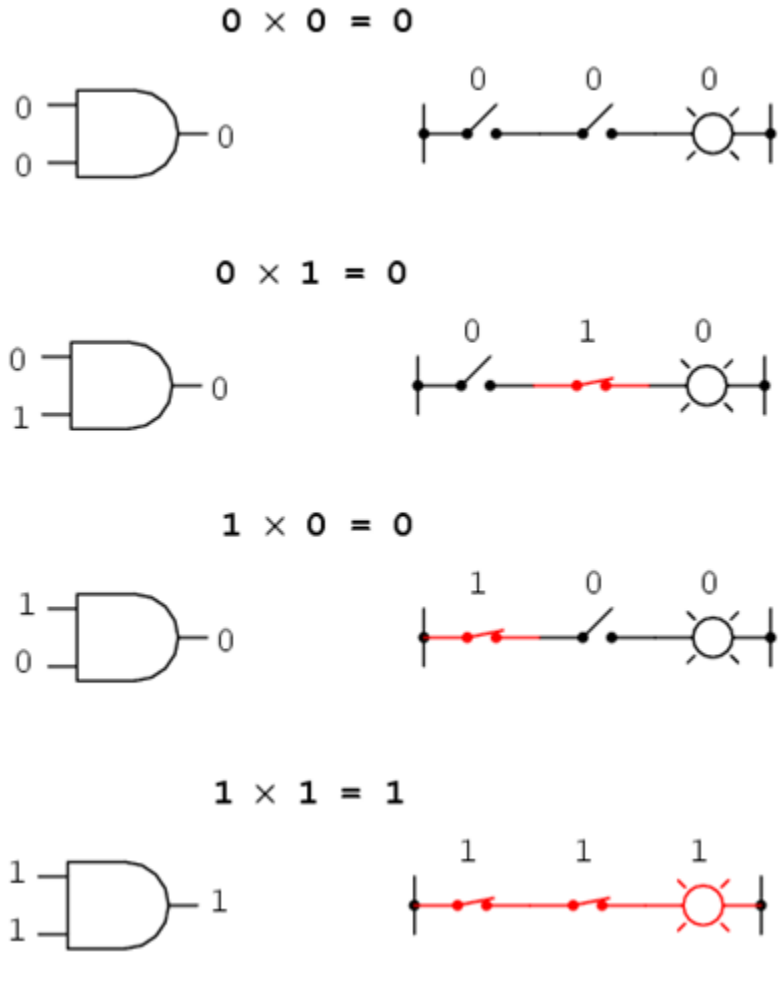


INHIBIT - Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDTIONING EVENT drawn to the right of the gate)

http://www.allaboutcircuits.com/vol_4/chpt_7/2.html

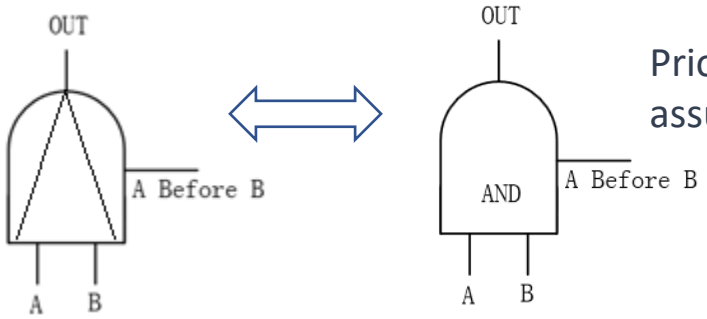
Boolean Logic



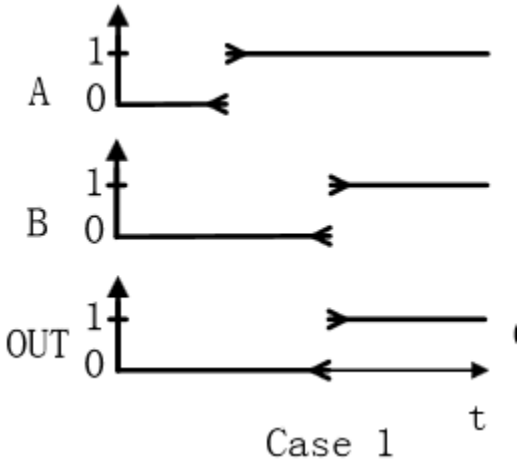


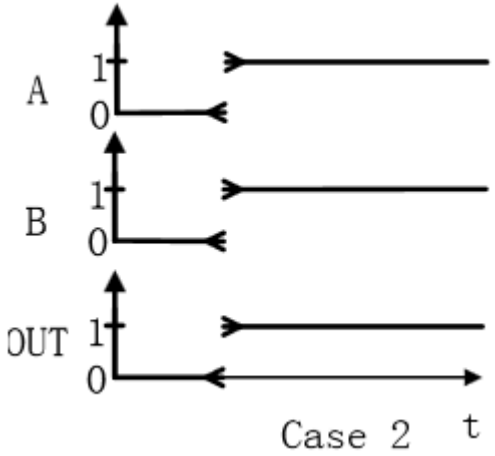
FTA Gate Logic

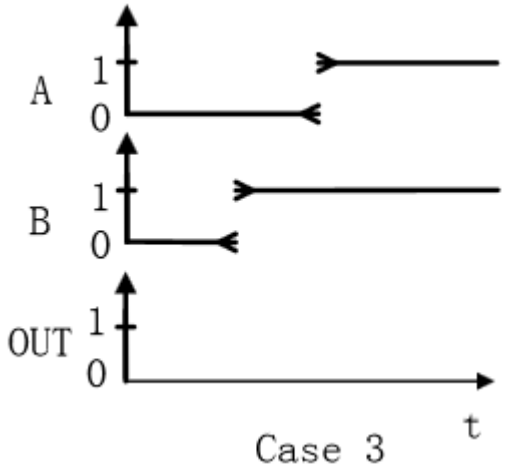
House event- External event – an event that is normally expected to occur. These events have a fixed probability of 0 or 1.



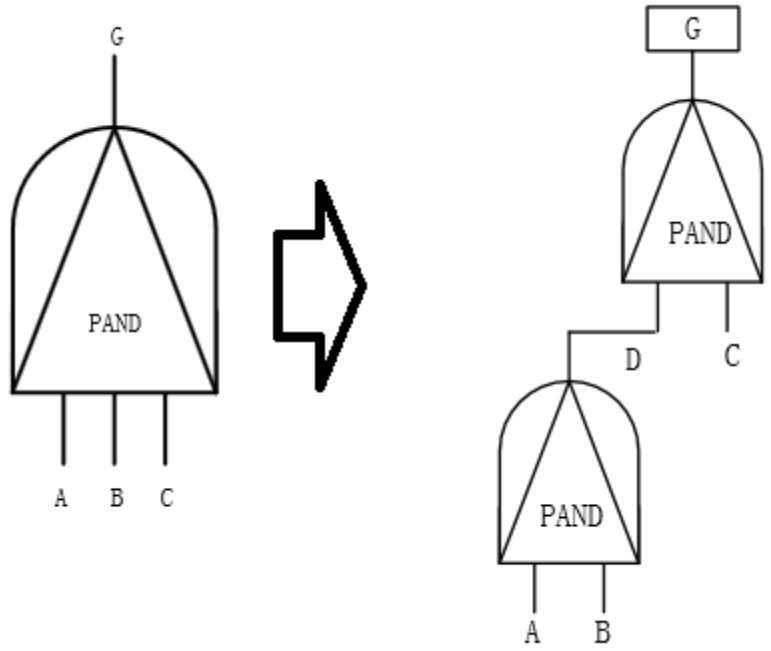
Priority AND (PAND) gate – ordered event, order is assumed from left to right.





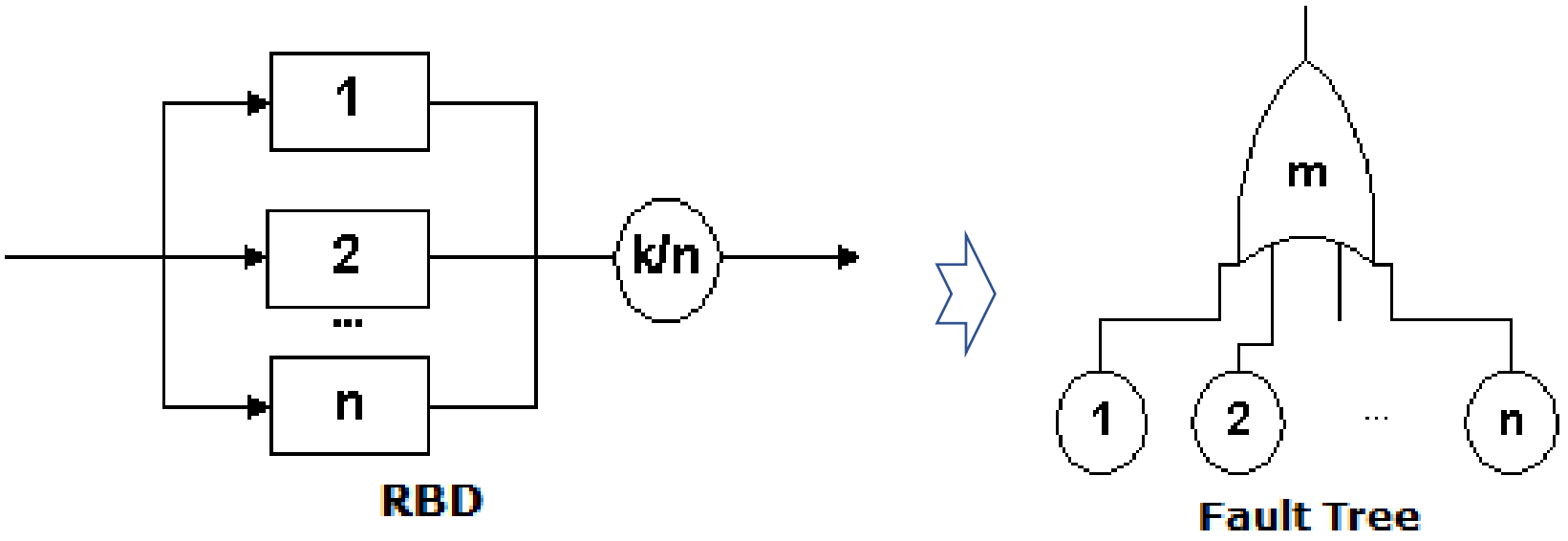


FTA Additional Symbols



FTA Examples

Example:
converting a Reliability Block Diagram (RBD) to a Fault Tree (FT)



some quantity (m) of all input events (qty = n) must occur

Cut Set

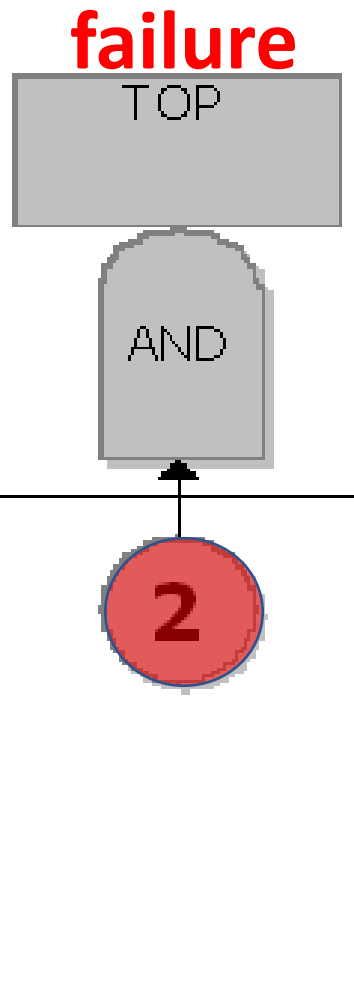
A cut set is a combination of basic events that can cause the top event.

An minimal cut set (MCS) is the smallest combination of basic events that result in the top event. The basic events are the bottom events of the fault tree. Hence, the minimal cut sets relate the top event directly to the basic event causes.

The set of MCSs for the top event represent all the ways that the basic events can cause the top event. A more descriptive name for a minimal cut set may be “minimal failure set.” The set of MCSs can not only be obtained for the top event, but for any of the intermediate events (e.g., gate events) in the FT.

Example

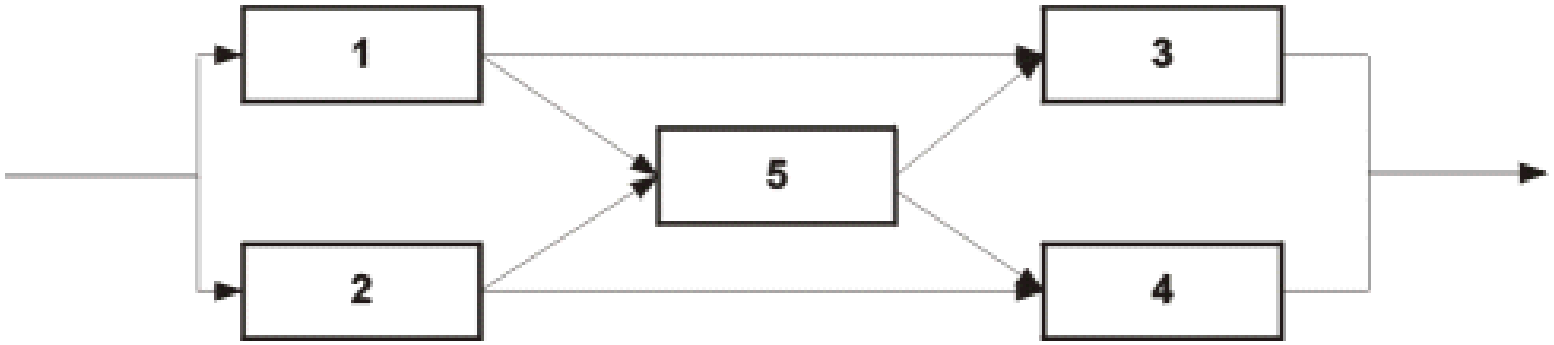
1	2	3	4	out(fail)
0	0	0	0	0
0	0	0	1	0
1	1	1	1	1



1	2	3	4	out(fail)
0	0	0	0	0
0	0	0	1	0
1	1	1	0	1
1	1	0	1	1
1	1	1	1	1

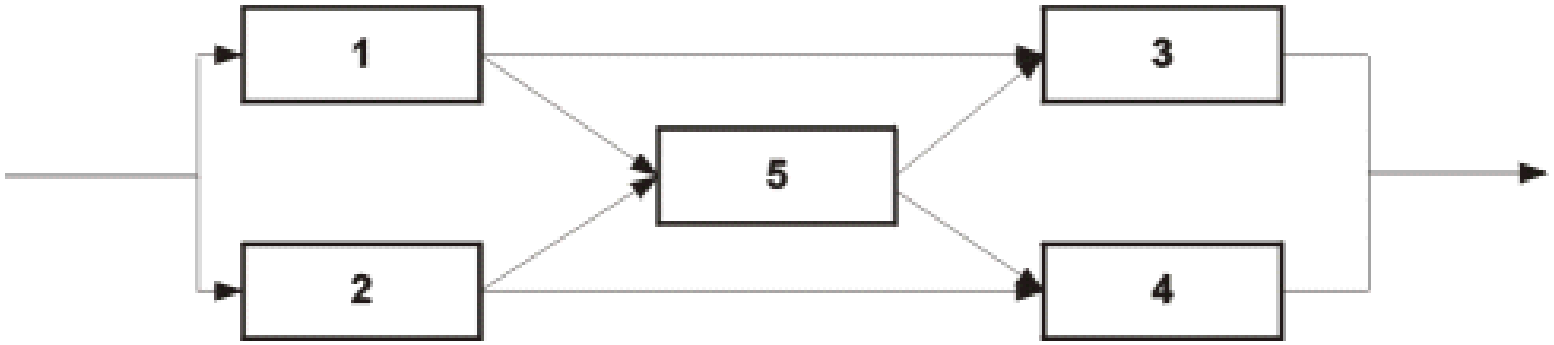
FTA Exercise

Exercise:
Converting a Reliability Block Diagram (RBD) to a Fault Tree (FT)



FTA Exercise

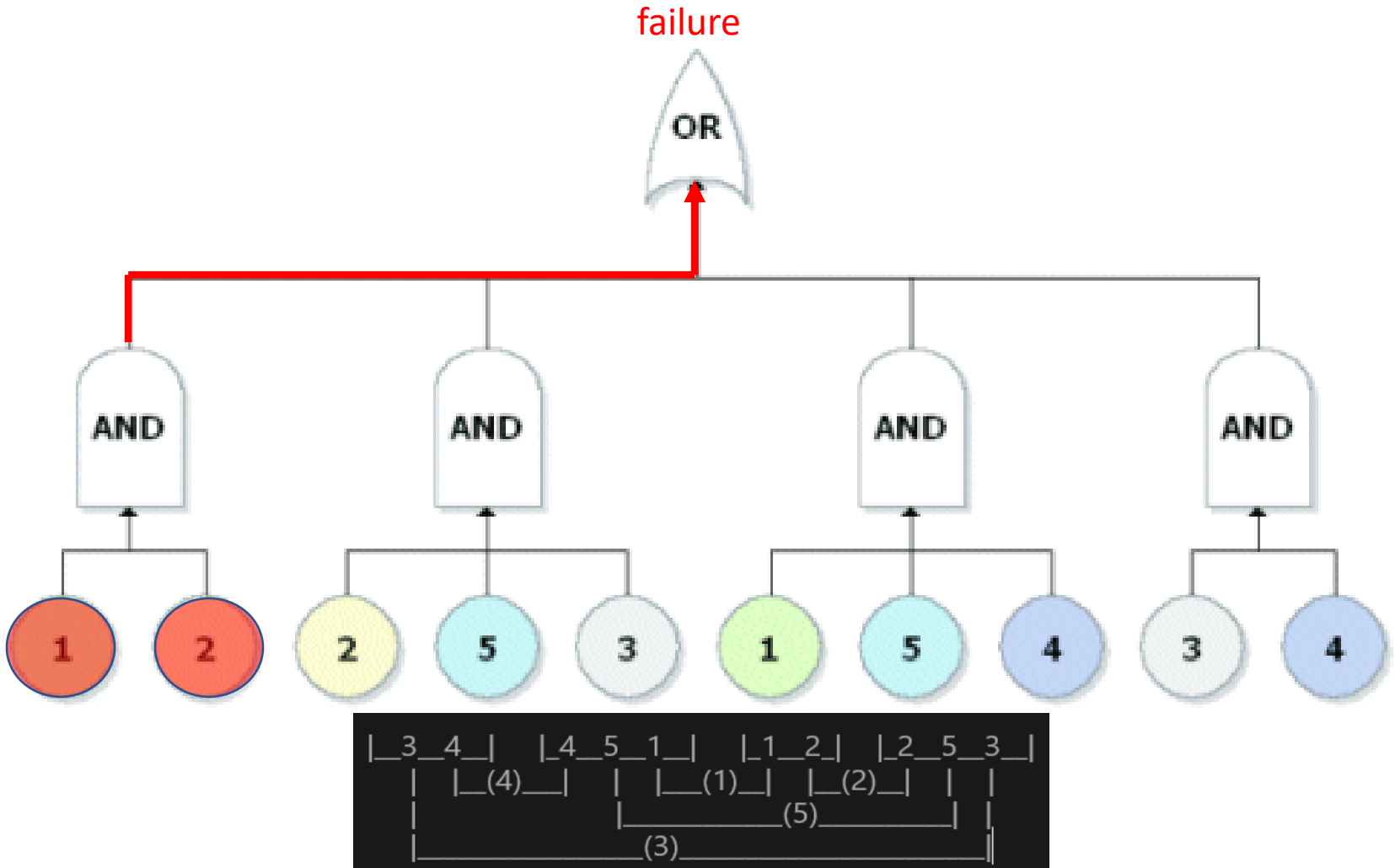
Exercise:
Converting a Reliability Block Diagram (RBD) to a Fault Tree (FT)



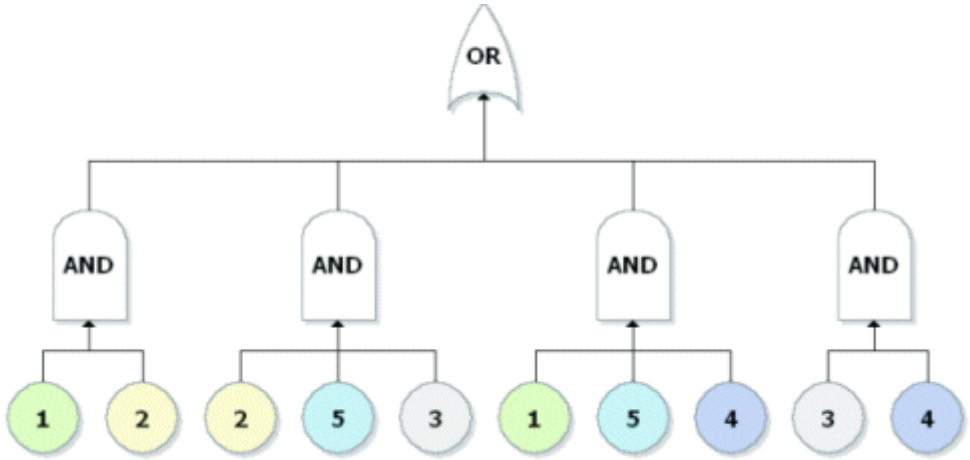
An inspection of the reliability-wise configuration of this system reveals that any of the following failures will cause the system to fail:
Failure of components 1 and 2.
Failure of components 3 and 4.
Failure of components 1 and 5 and 4.
Failure of components 2 and 5 and 3.

Exercise

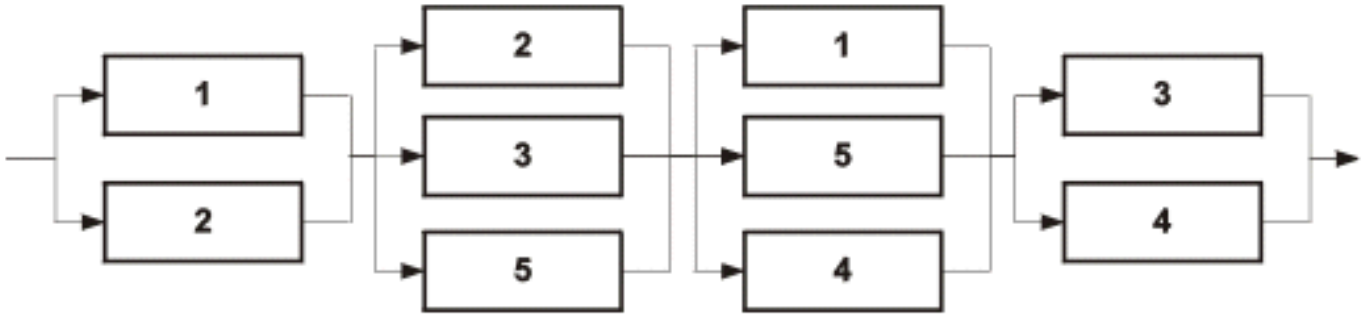
"minimal cut sets” (1 AND 2) OR (3 AND 4) OR (1 AND 5 AND 4) OR (2 AND 5 AND 3)



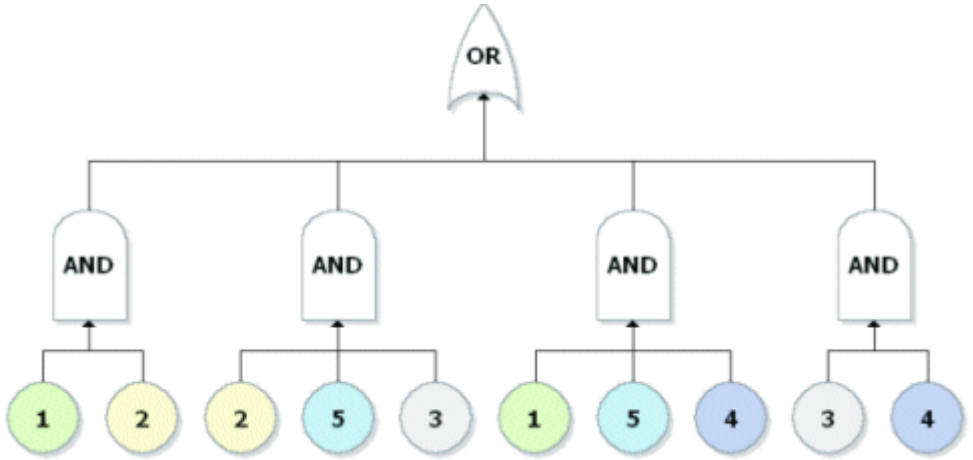
Cut Sets



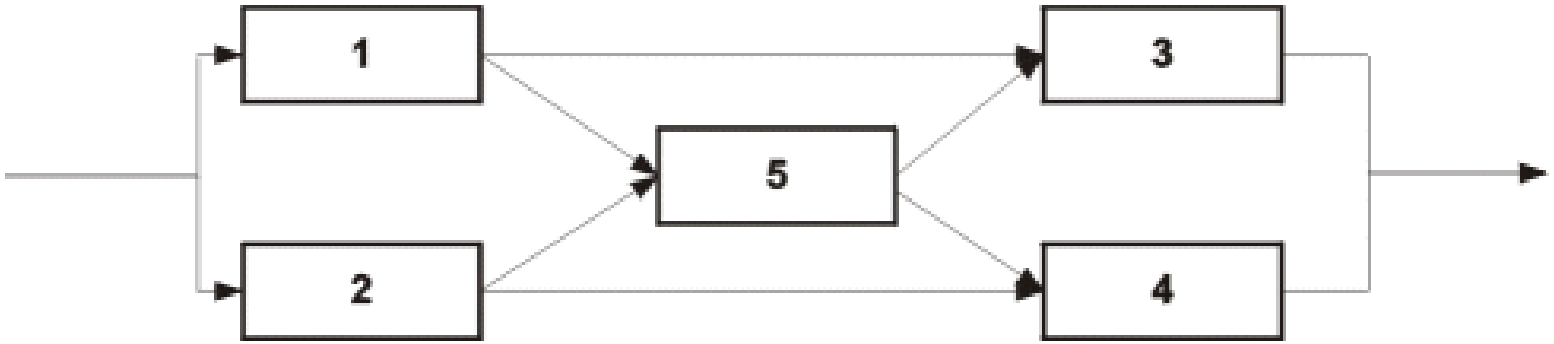
The above configuration in a reliability block diagram. This diagram also requires the use of more than one block in the diagram to represent the same component. Blocks with the same number in the diagram are identical.



Cut Sets



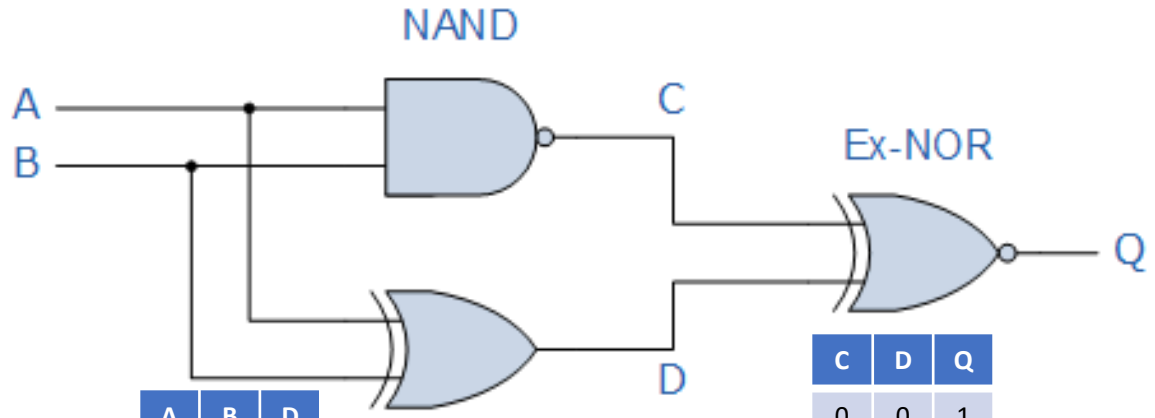
The above configuration in a reliability block diagram. This diagram also requires the use of more than one block in the diagram to represent the same component. Blocks with the same number in the diagram are identical.



Boolean Algebra Review

Construct a Truth Table for the logical functions at points C, D and Q in the following circuit and identify a single logic gate that can be used to replace the whole circuit.

A	B	C
0	0	1
0	1	1
1	0	1
1	1	0



A	B	D
0	0	0
0	1	1
1	0	1
1	1	0

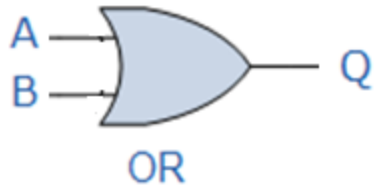
C	D	Q
0	0	1
0	1	0
1	0	0
1	1	1

Truth Table

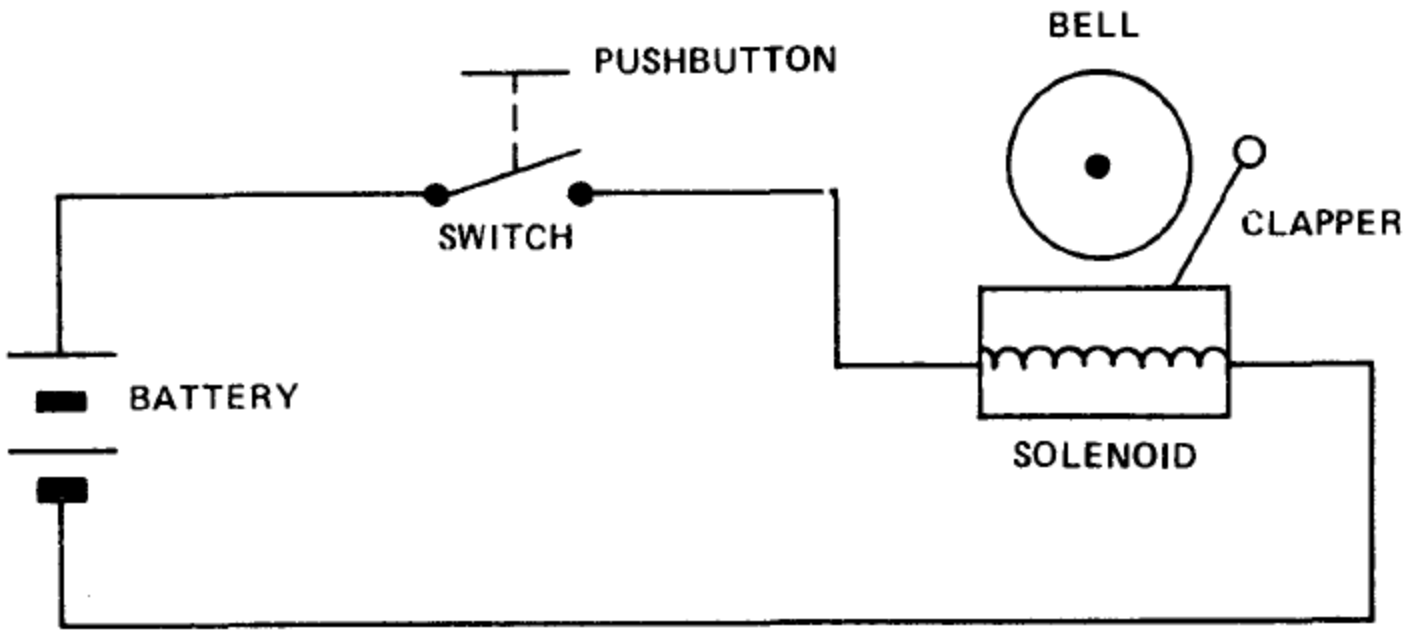
Inputs		Output at		
A	B	C	D	Q

Truth Table

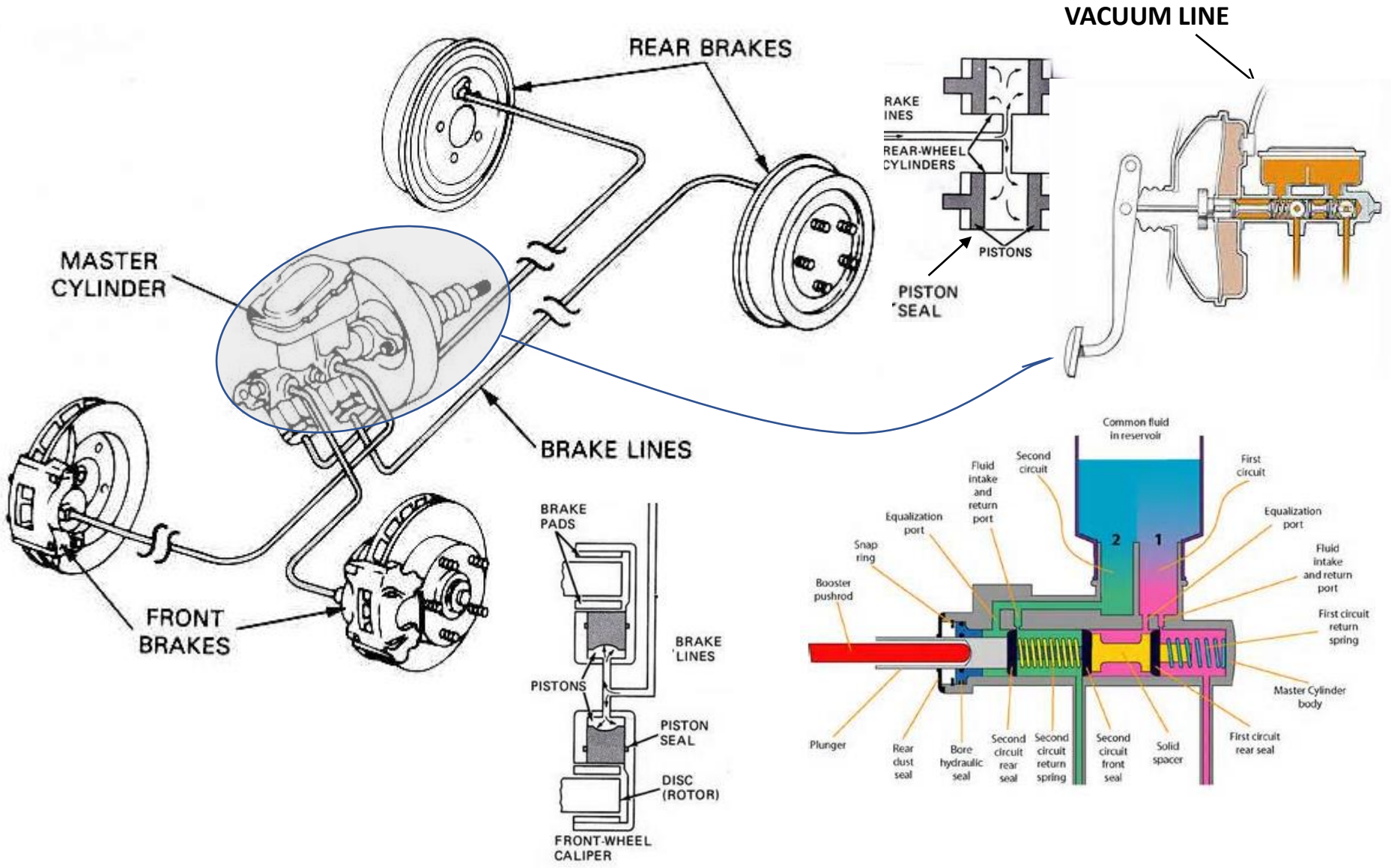
Inputs		Output at		
A	B	C	D	Q
0	0	1	0	0
0	1	1	1	1
1	0	1	1	1
1	1	0	0	1



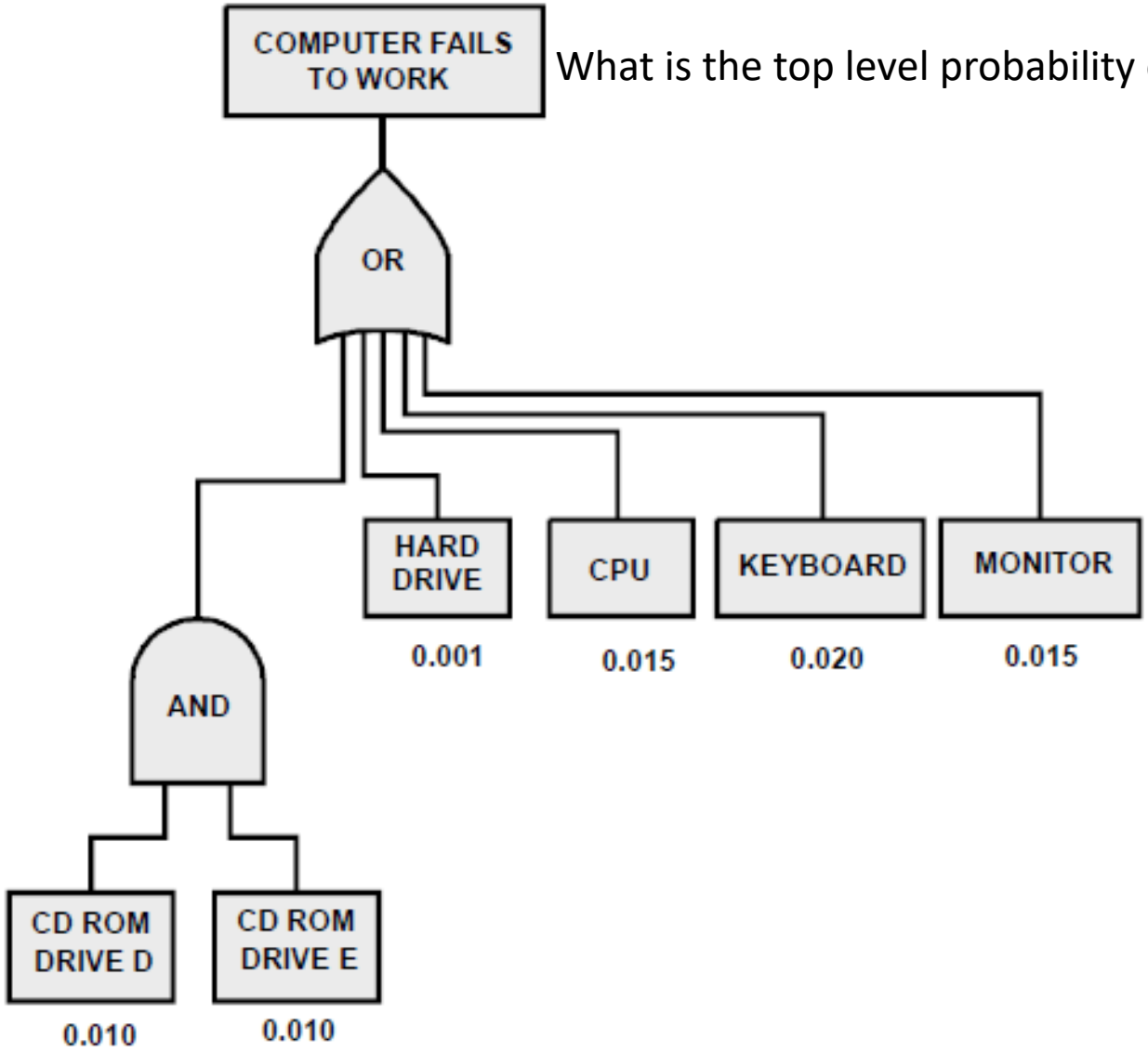
Exercise



Exercise

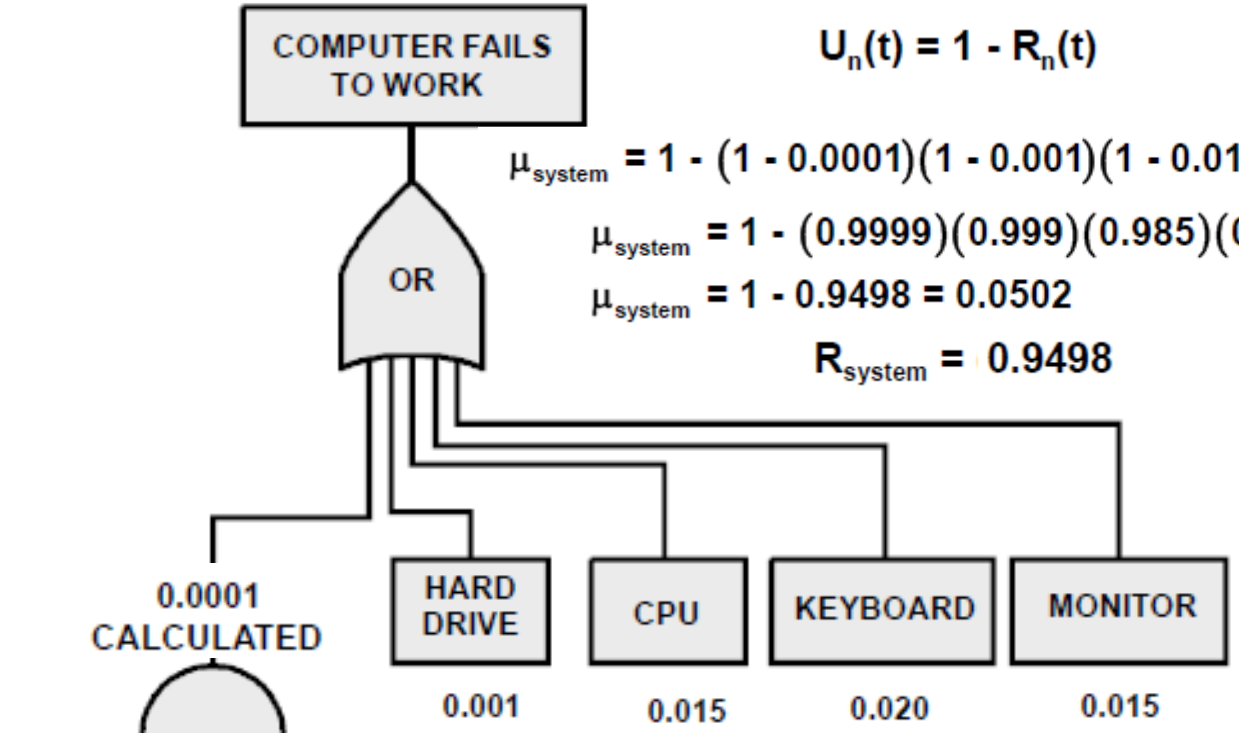

REAR BRAKES
MASTER CYLINDER
BRAKE LINES
FRONT BRAKES
RAKE INES
REAR-WHEEL CYLINDERS
PISTONS
PISTON SEAL
VACUUM LINE
BRAKE PADS
BRAKE LINES
PISTONS
PISTON SEAL
DISC (ROTOR)
FRONT-WHEEL CALIPER
Common fluid in reservoir
Second circuit
First circuit
Fluid intake and return port
Equalization port
Snap ring
Booster pushrod
Plunger
Rear dust seal
Bore hydraulic seal
Second circuit rear seal
Second circuit return spring
Second circuit front seal
Solid spacer
First circuit rear seal
Master Cylinder body
First circuit return spring
2
1

Exercise: Fault Tree



What is the top level probability of failure?

Exercise: Fault Tree



$U_n(t) = 1 - R_n(t)$

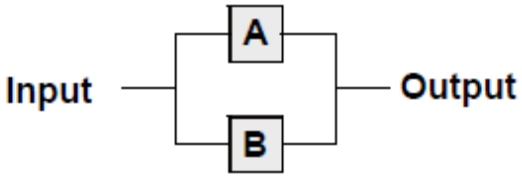
$\mu_{system} = 1 - (1 - 0.0001)(1 - 0.001)(1 - 0.015)(1 - 0.020)(1 - 0.015)$

$\mu_{system} = 1 - (0.9999)(0.999)(0.985)(0.980)(0.985)$

$\mu_{system} = 1 - 0.9498 = 0.0502$

$R_{system} = 0.9498$

Active Parallel Systems

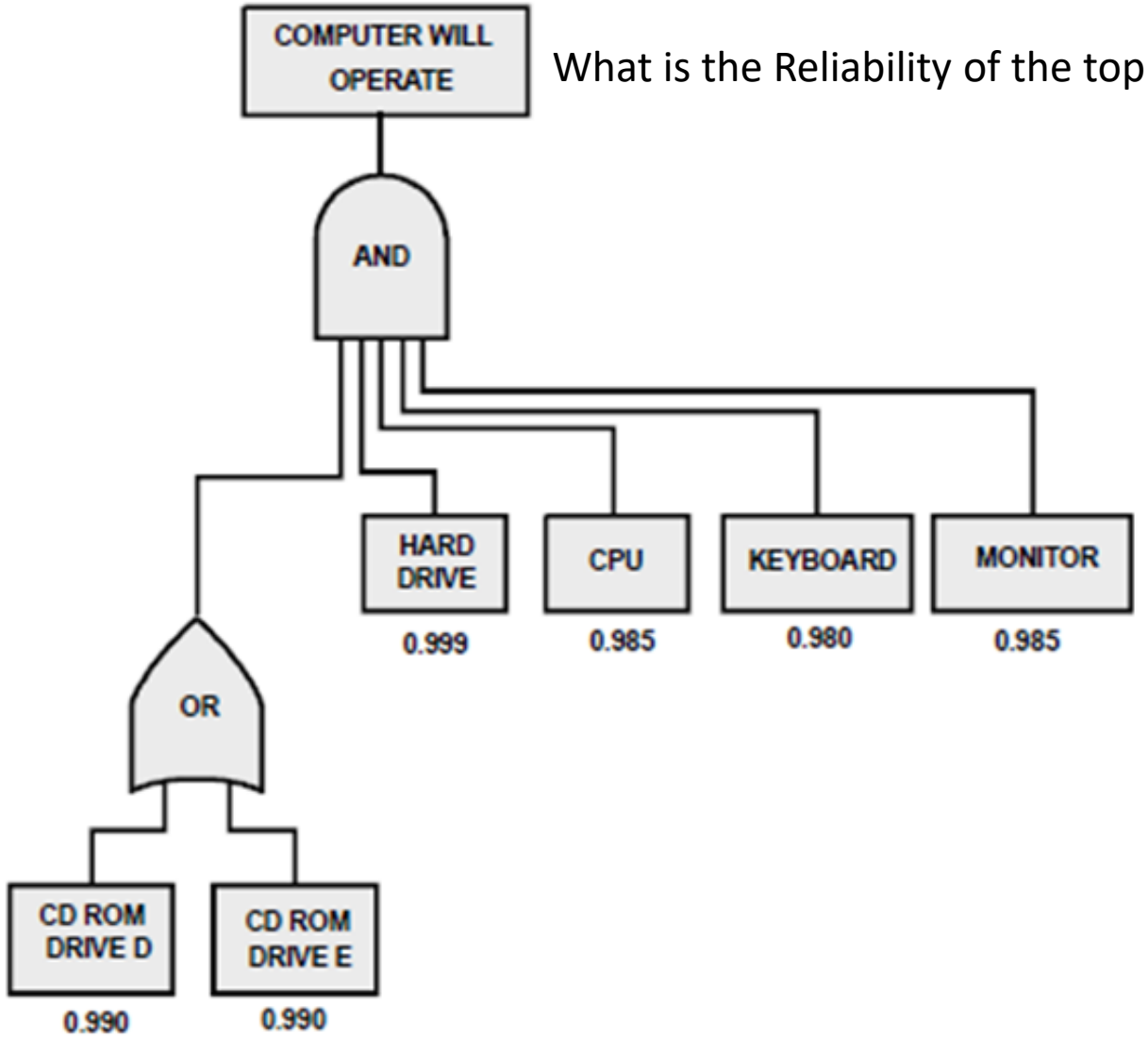


$R_{(system)}(t) = R_A + R_B - R_A R_B$

$U(t) = 1 - R(t)$

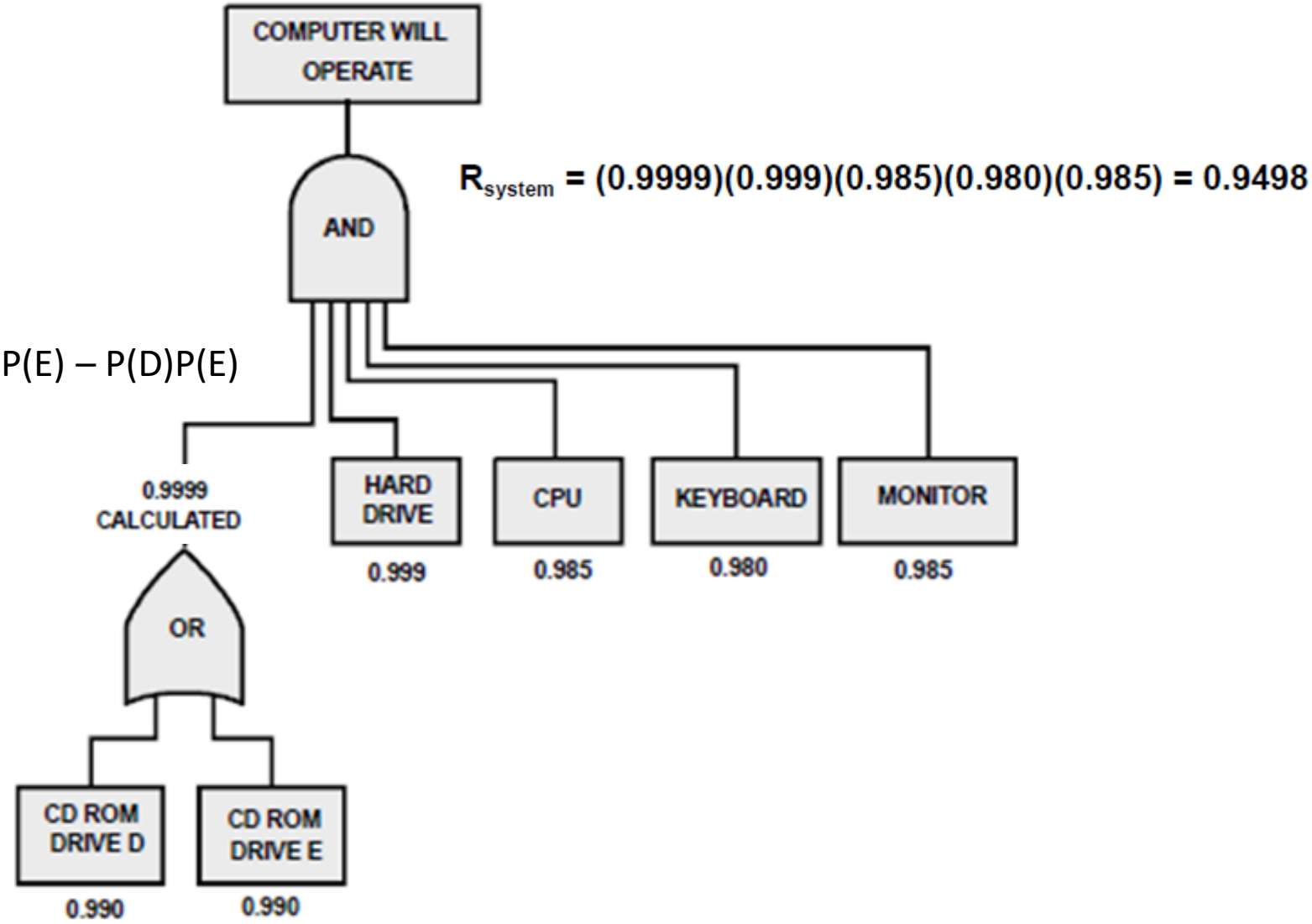
$R(t) = 1 - [U_A(t) \times U_B(t)]$

Exercise: Success Tree

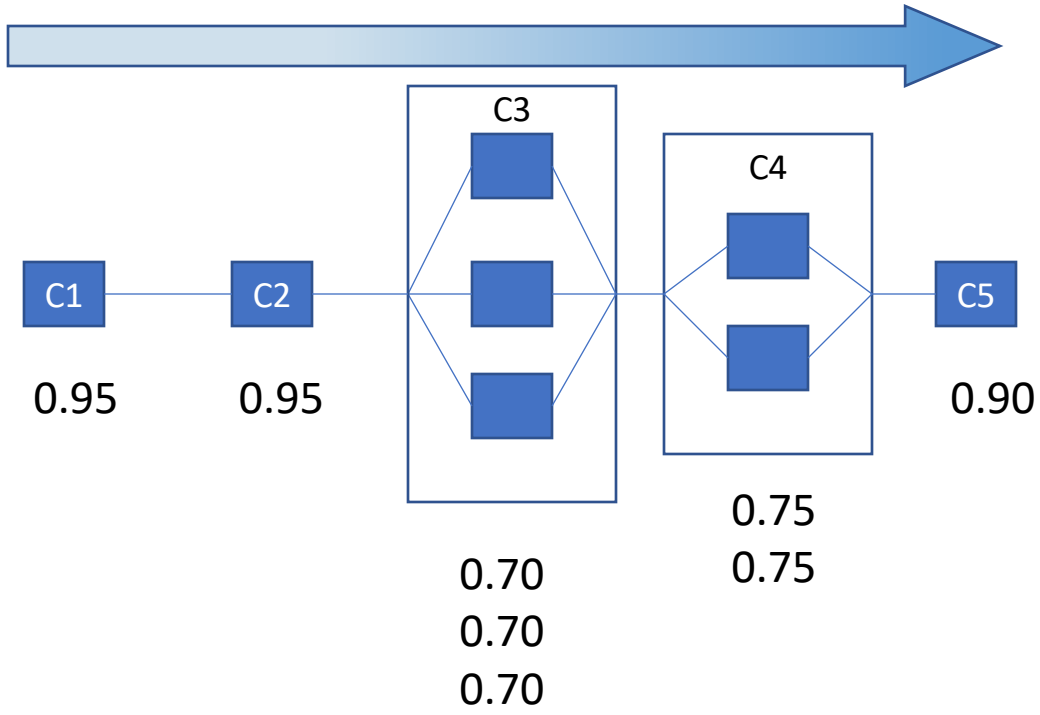


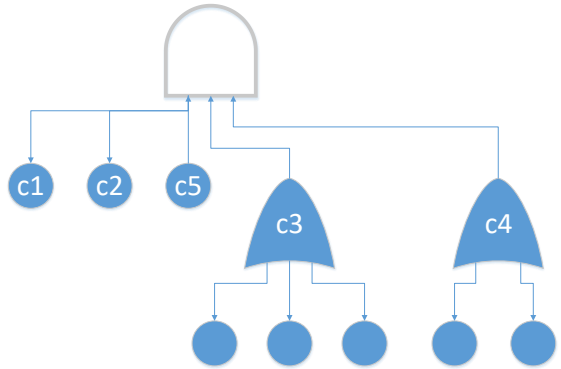
What is the Reliability of the top level event?

Exercise: Success Tree



Series - Parallel





C1 −→ C2 −→ C3 −→ C4 −→ C5

P(C1) × P(C2) × P(at least 1 C3) × P(at least 1 C4) × P(C5)

$$\text{Rel} = .95 \times .95 \times (1 - .3^{3}) \times (1 - .25^{2}) \times .9 = 0.7409243$$

0.973 0.9375

Failure Modes and Effects Analysis (FMEA)

Timing Is Everything

- Initiate FMEAs Early in Development Phase of Product Designs or Processes

- Most Benefits Achieved with Early Implementation
  - Design-Out Potential Failure Modes by Eliminating Root Causes
  - Reduce Seriousness of Failure Mode if Elimination Not Possible
  - Reduce Occurrence of Failure Mode

Failure Modes and Effects Analysis (FMEA)

Item	Potential failure mode	Effects	Sev	Causes	Occ	Current controls	Det	RPN	Recom'ed actions	Responsible and date	Action	Results			
											Actions taken	Sev	Occ	Det	RPN
A29	Pin bends	V16 sags	6	Low carbon	1	Hardness check	8	48	Change spec. to supplier	Jim Hzn. 8/21/12	Spec. chgd.	6	1	2	12

Current Controls do not make a distinction between Prevention and Detection
Prevention and Detection for a DFMEA have different meaning than for a PFMEA

In the above example the DET is changed from an 8 to a 2 based upon the action: change spec to supplier
It is not clear as to what the connection is between the Recommended Actions and the Cause And/or Controls. Furthermore, it is not clear as to whether the Hardness Check is being implemented or was always there.

Failure Modes and Effects Analysis (FMEA)

Functional

Function/Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s) / Mechanism(s) of Failure	Occur	Current Controls - Prevention	Current Controls - Detection	Detect	S.O.	R.P.N.	Recommended Action(s)
Steering												
Safety assist systems												
Lane Keeping Assist	Fails to meet customer needs	Loss of customers, brand impact	9		**Incomplete requirements**	5	**Project centric requirements management**			45		

Design

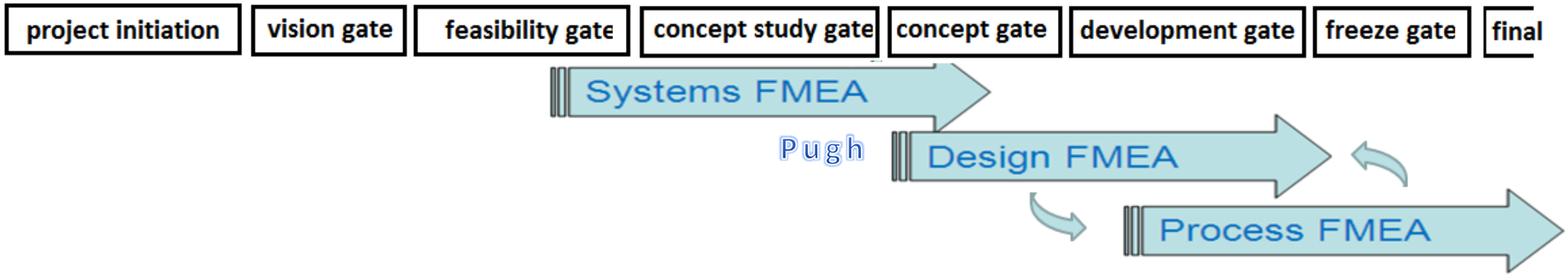
Function/Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s) / Mechanism(s) of Failure	Occur	Current Controls - Prevention	Current Controls - Detection	Detect	S.O.	R.P.N.	Recommended Action(s)
Steering												
Lane Keeping Assist												
R1: Activation of counter steering	unrequested activation	unintended trajectory - potential for safety issue	9		Software bug	5	software testing - coverage and depth	fault injection, simulation, etc.	3	45	**135**	

Process

Function/Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s) / Mechanism(s) of Failure	Occur	Current Controls - Prevention	Current Controls - Detection	Detect	S.O.	R.P.N.	Recommended Action(s)
attach part A to part B												
R1: align and torque to spec	incorrect alignment	C: quality impression	3		human error	5	W. I.	visual insp.	8	15	120	
		M: rework in station impact value stream	8		human error	5	W.I.	visual insp.	8	40	320	

FMEA training -- timing a FMEA

- When, exactly, do I start a
  Functional (System) FMEA?
  Design FMEA?
  Process FMEA?



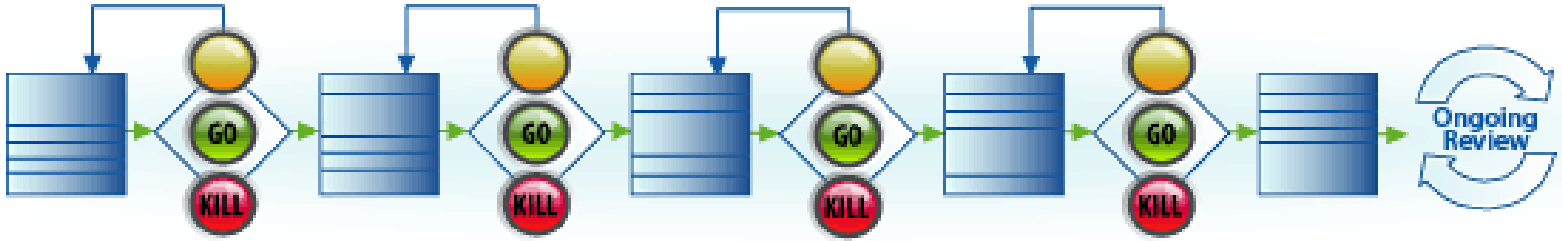
Strategic objectives

- Develop FMEA as a core competency
- Develop a cadre of competent FMEA facilitators
- Transition from a reactive to a preventive organization

proactive

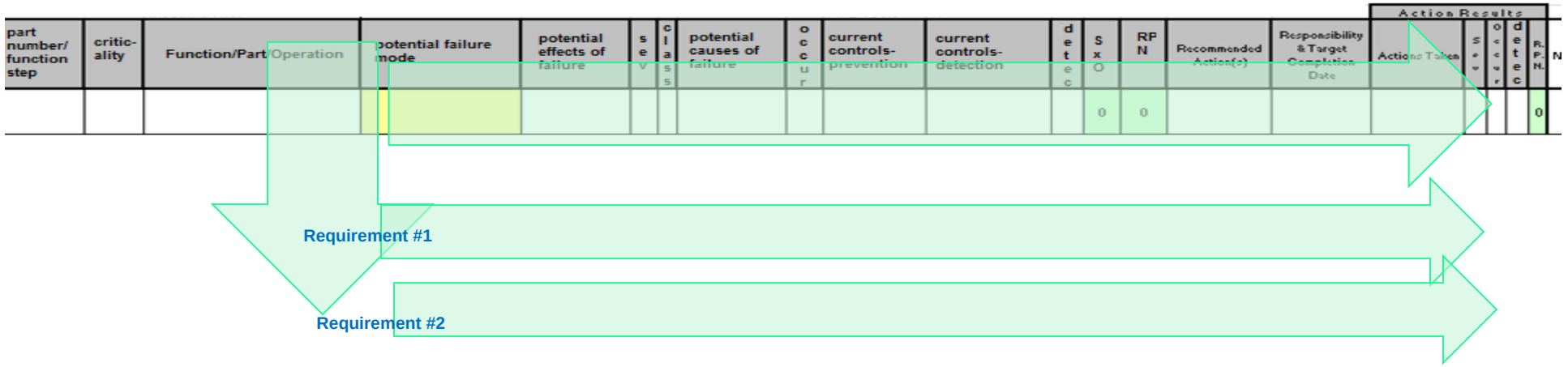
Preventive actions

reactive



Front End Loading

Failure Modes and Effects Analysis (FMEA)



Failure Modes and Effects Analysis (FMEA)

Phase I: Getting Started

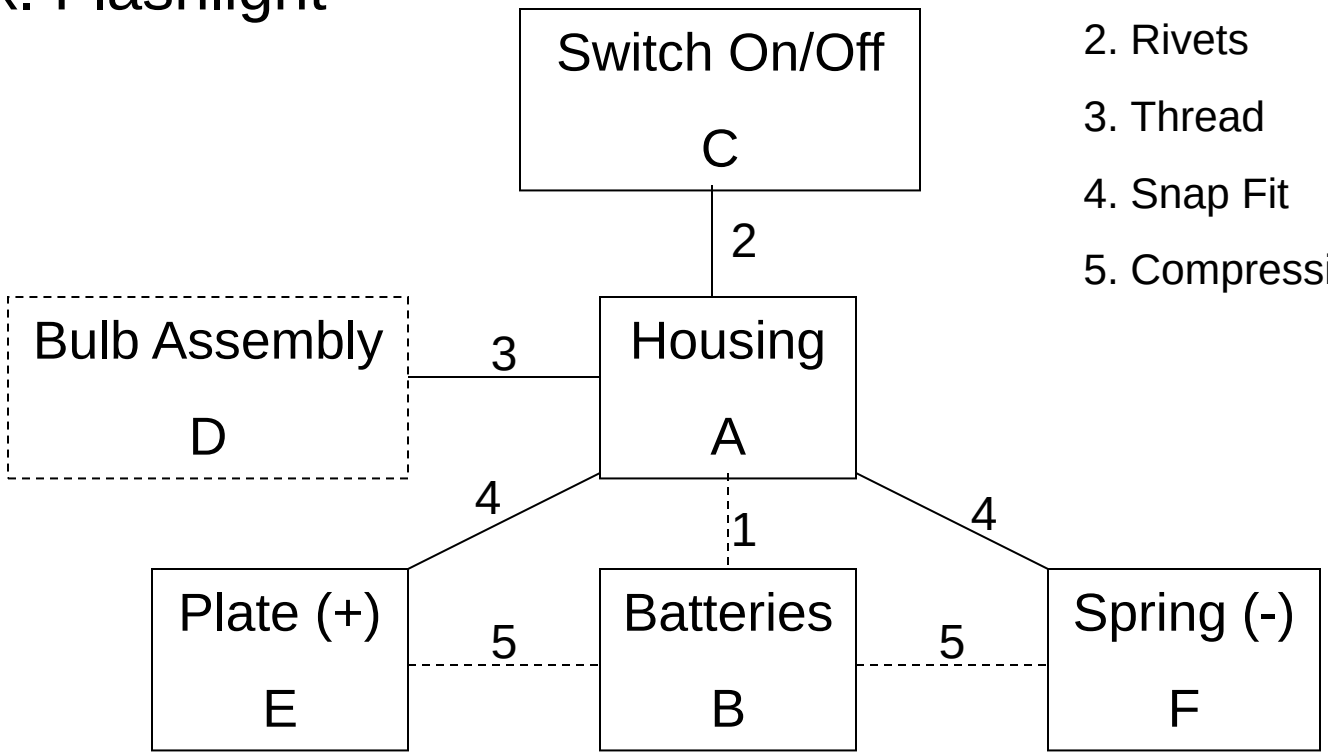
- Examples of Block Diagram for System, Subsystem, Components

  - Four Types
    - Relational
    - Hierarchy
    - Functional
    - Reliability
    - PFD

Failure Modes and Effects Analysis (FMEA)

Phase I: Getting Started

- Relational Block Diagram
  - Ex. Flashlight



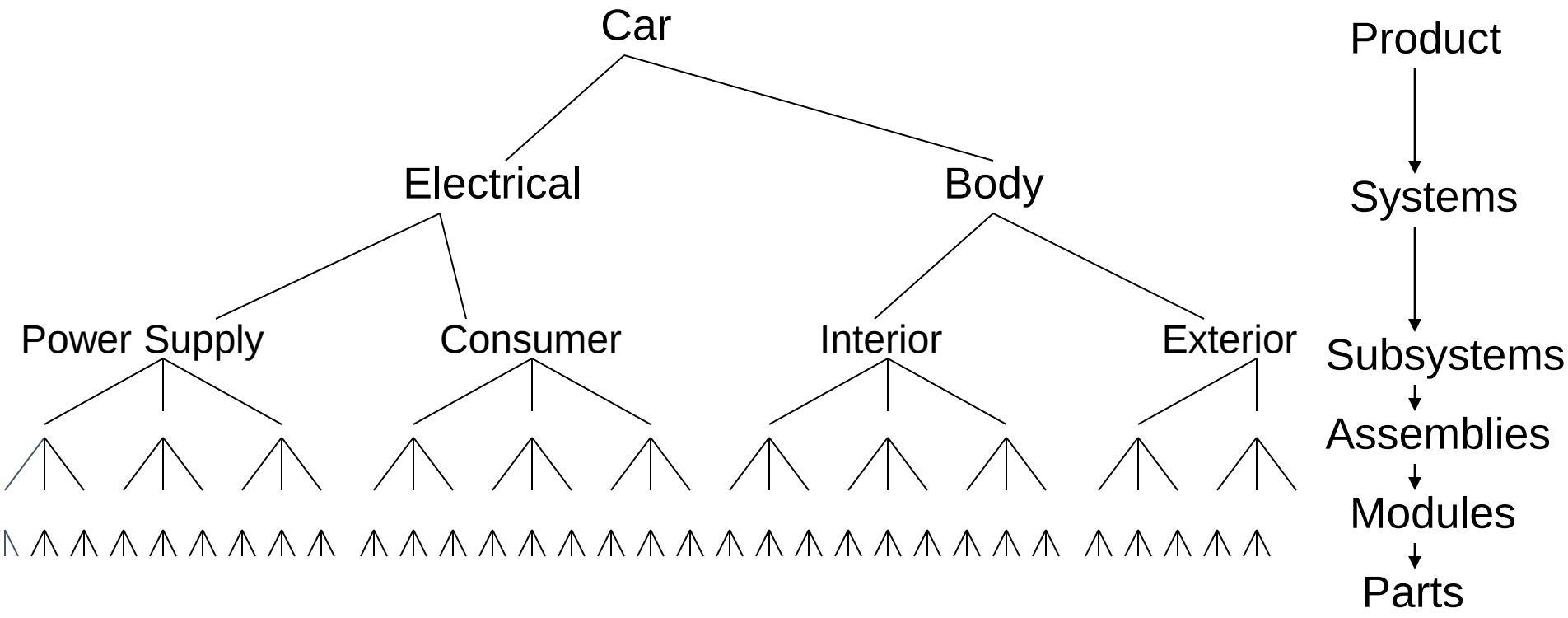
Attaching Method

1. Skip Fit
2. Rivets
3. Thread
4. Snap Fit
5. Compressive Fit

Failure Modes and Effects Analysis (FMEA)

Phase I: Getting Started

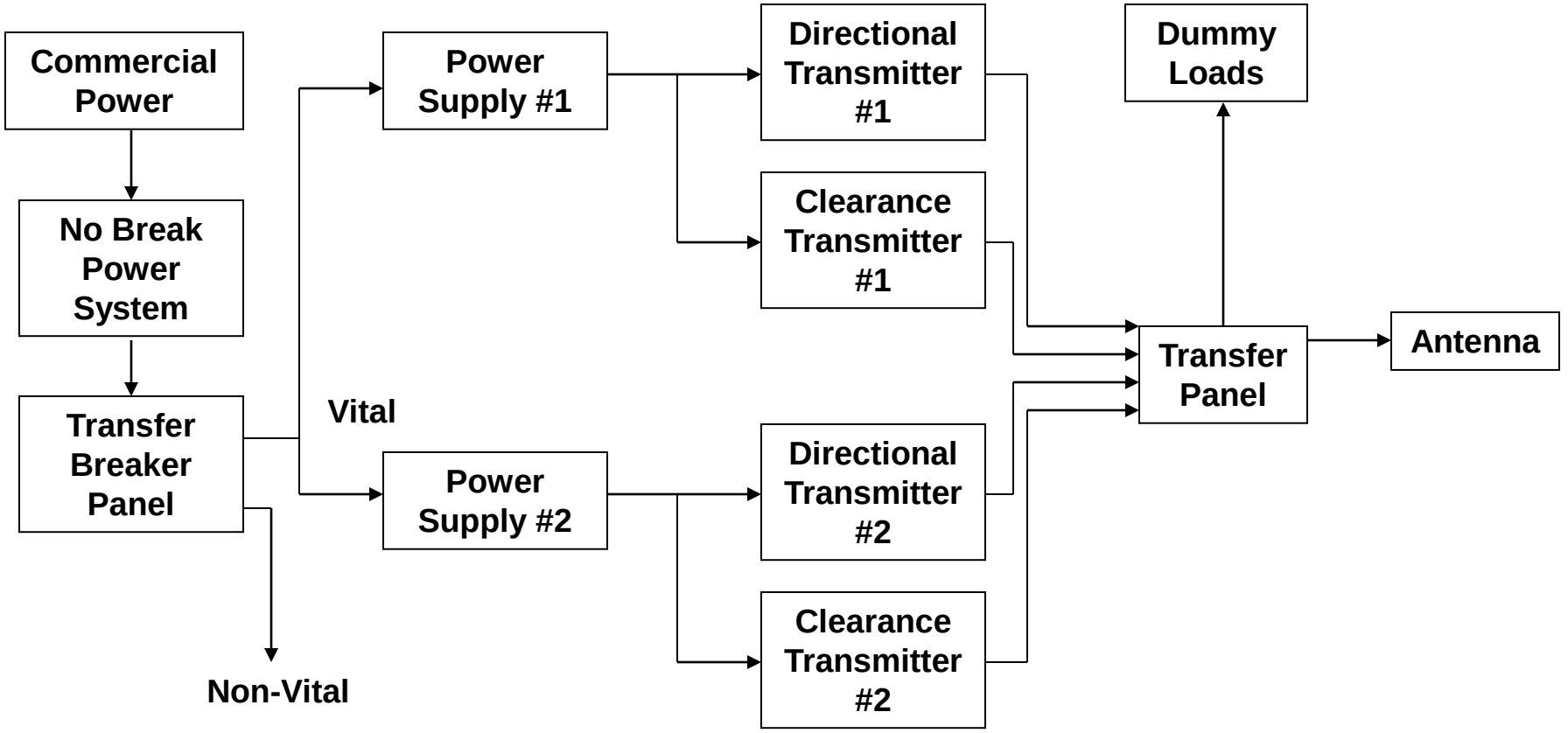
- Hierarchy Block Diagram
  - Ex. Car



Failure Modes and Effects Analysis (FMEA)

Phase I: Getting Started

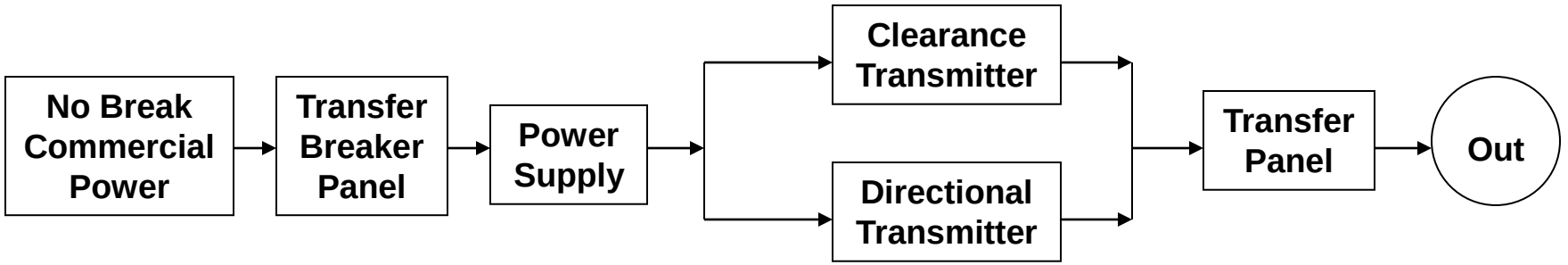
- Functional Block Diagram



Failure Modes and Effects Analysis (FMEA)

Phase I: Getting Started

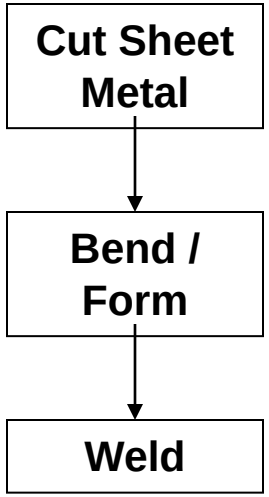
- Reliability Block Diagram



Failure Modes and Effects Analysis (FMEA)

Phase I: Getting Started

- Process Flow Diagram

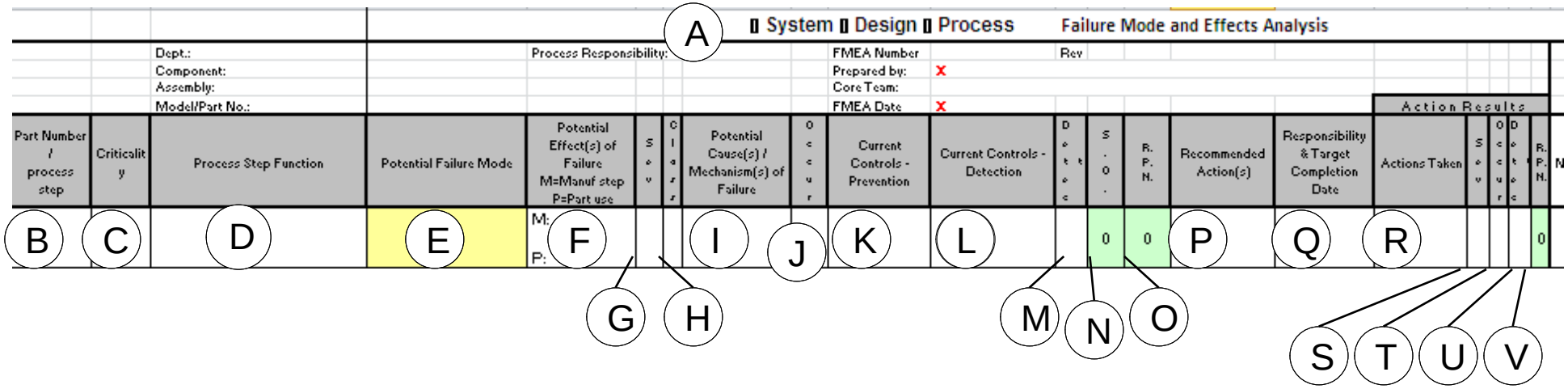


FMEA

Performing a ***FMEA***

Phase II: Step A

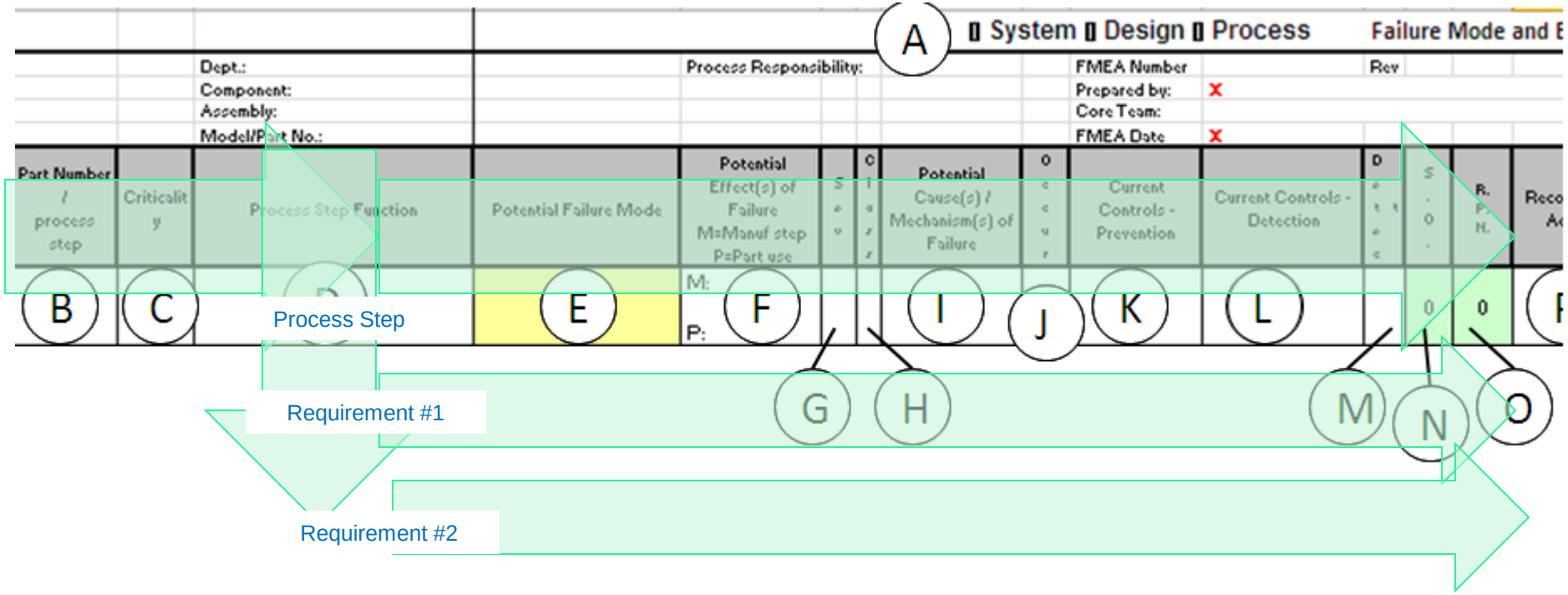
Process (Design) FMEA Header



FMEA

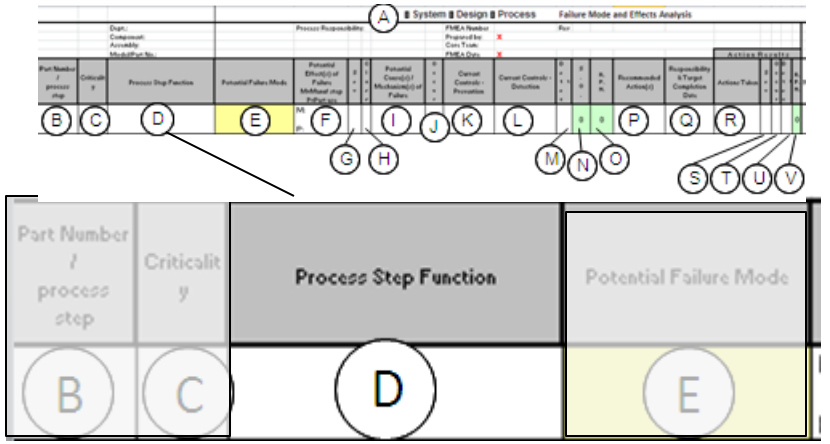
Performing a **FMEA**

Phase II: Populating the FMEA and Ranking the RPNs



FMEA

Performing a ***FMEA***



Phase II: Step D

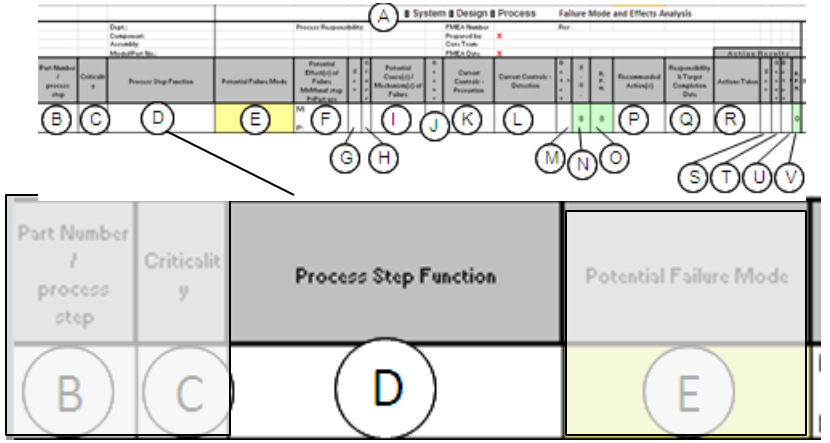
Design FMEA

Step D: List Each System, Subsystem, Component and Their Functions

- List Each Item Separately, Include Available P/Ns
- List Each Function(s) Individually and Concisely, Include Information (Metrics/Measurables) Regarding the Operating Environment
- List the requirements relative to the functions

FMEA

Performing a ***FMEA***



Phase II: Step D

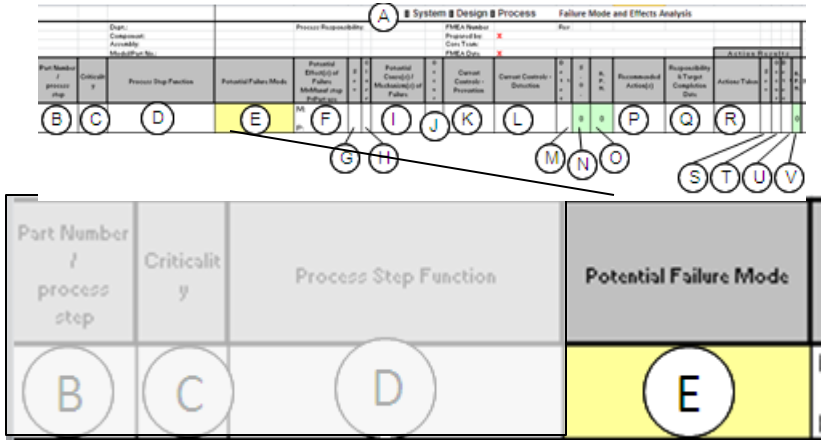
Process FMEA

Step D: List Each Process Step (and the Requirements of the Process Output)

- Describe Each Process Step Separately and Concisely
- Process Step Requirements Listed Independently
- Review Performance, Material, Process, Environmental, Safety, Etc. Standards

FMEA

Performing a ***FMEA***



Phase II: Step E

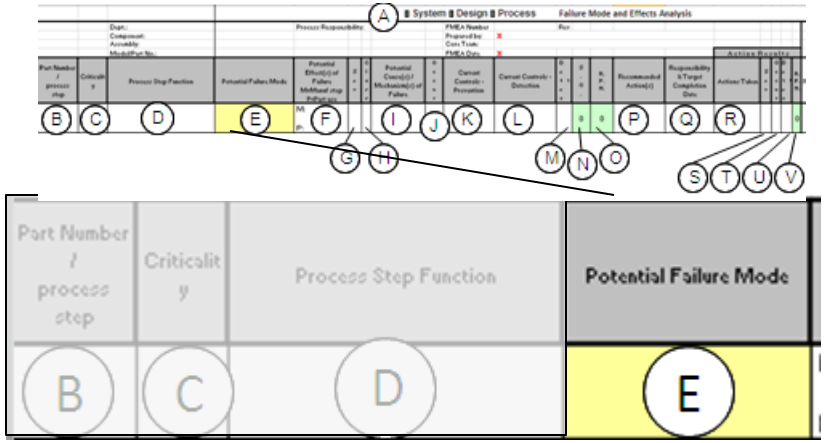
Design FMEA

Step E: List All the Potential Failure Modes (PFMs) for Each Function

- Questions to Answer:
  - How can the item/part fail to meet requirements?
  - What would a customer (internal or external) consider objectionable?
  - Include non-functional requirements
- Describe in “Physical/Technical” Terms, Not as a Symptom
- PFMs may be a Cause of a PFM in a Higher-Level System, or an Effect of a PFM in a Lower-Level Component

FMEA

Performing a ***FMEA***



Phase II: Step E

Process FMEA

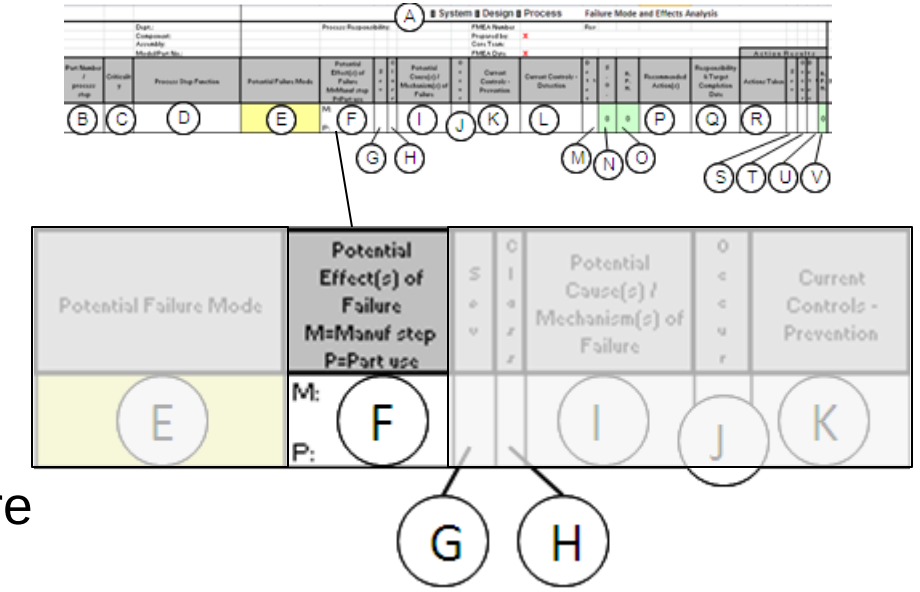
Step E: List All the Potential Failure Modes (PFMs) for Each Process Step

- Questions to Answer:
  - How can the item/part fail to meet requirements?
  - What would a customer (internal or external) consider objectionable?
- Describe in “Physical/Technical” Terms, Not as a Symptom
- PFM Describes Non-Conformance at that Specific Operation

FMEA

Performing a ***FMEA***

Phase II: Step F



Process FMEA

Step F: List All the Potential Failure (PFMs) for Each Process Step

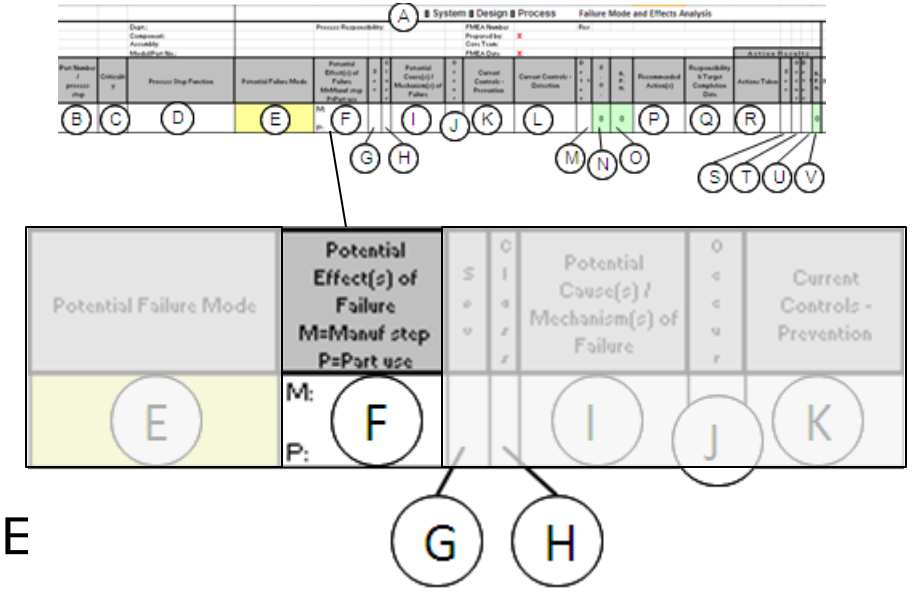
- Assume Incoming Parts/Materials Meet Requirements. Exception: Historical Data Indicates Deficiencies in Incoming Parts

- PFMs may be a Cause of a PFM in a Subsequent Operation, or an Effect of a PFM in a Previous Operation

FMEA

Performing a ***FMEA***

Phase II: Step F



Design and Process FMEA

Step F: List the Potential Effect of E

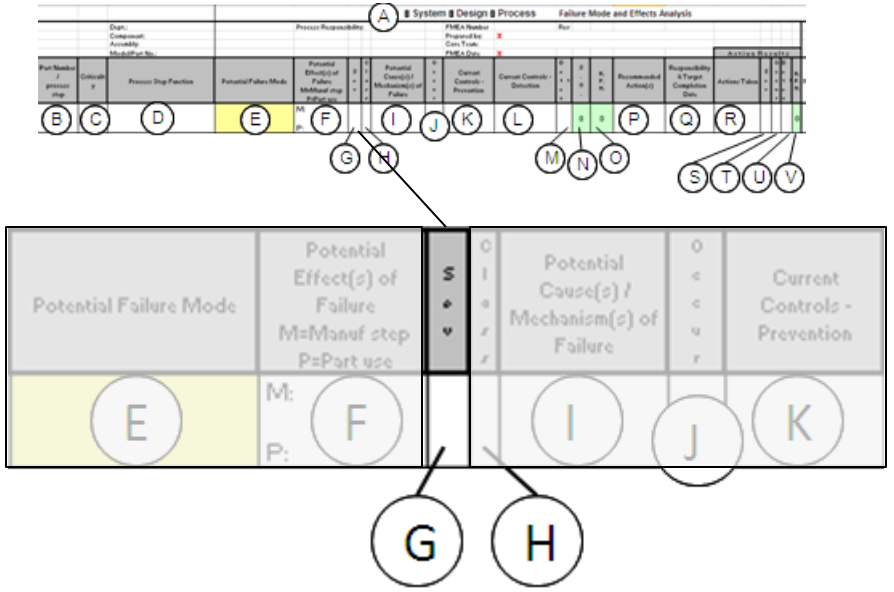
- Enter Separately the Effect of Each PFM on Product Performance (and Manufacturability)
- Describe Effects in Specific Terms of What Customer Might Notice or Experience
- Consider Both Internal and External Customers
- State Effects on Safety Clearly

FMEA

Performing a ***FMEA***

Phase II: Step G

Design and Process FMEA



Step G: Assign a Severity Ranking

- Rank the Most Serious Effect for a Given PFM
- Ranking Scale of 1 - 10
- Do Not Further Analyze PFMs with Severity Rank of 1
- Severity Ranking Can Only Be Reduced Through Design Changes or Process Changes

FMEA

Performing a ***FMEA***

Phase II: Step G

Design FMEA

Rank	Severity
1	Customer will probably not even notice the failure.
2-3	Slight customer annoyance.
4-6	Causes some customer dissatisfaction. Customer is uncomfortable or annoyed.
7-8	High degree of dissatisfaction due to nature of the failure. Inoperable product or process subsystem. Does not involve safety.
9-10	PFM affects safe product or process operation and/or involves noncompliance with government and/or industry regulation.

Process FMEA

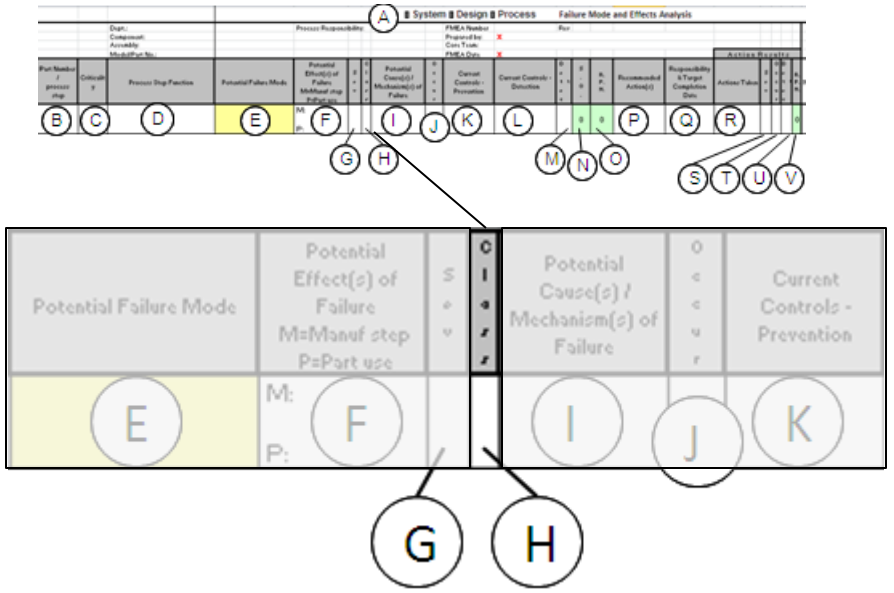
Rank	Severity
1	No discernable effect.
2-3	Slight customer annoyance. Some in-station rework may be required.
4-5	Causes some customer dissatisfaction. Some product may need to be reworked in-line but outside the workstation.
6-7	Causes substantial customer dissatisfaction to the point where a formal complaint may be registered. Some product may have to be scrapped.
8-9	Causes serious downstream process disruption and customer dissatisfaction. May affect on time delivery or lead time. Will likely result in significant scrap or performance issues.
10	Customer is extremely dissatisfied. Major performance attributes affected and significant process downtime is likely. May involve product recall. Severe safety implications.

FMEA

Performing a ***FMEA***

Phase II: Step H

Design and Process FMEA



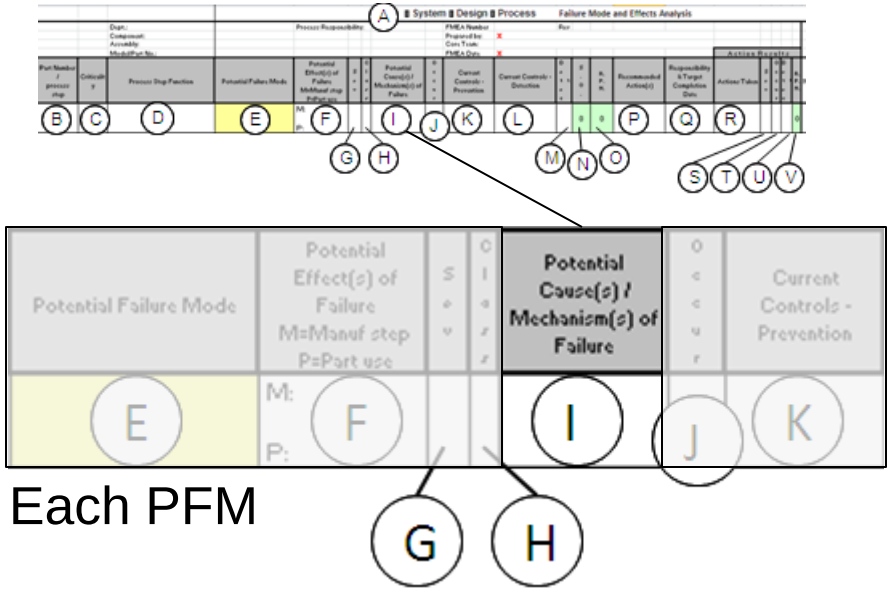
Step H: Assign a Class (as Appropriate)

- Classify Any Special Product or Process Characteristics (Critical, Key, Major, Significant) for the Component That May Require Additional Design or Process Controls

FMEA

Performing a ***FMEA***

Phase II: Step I



Design and Process FMEA

Step I: List All Potential Causes for Each PFM

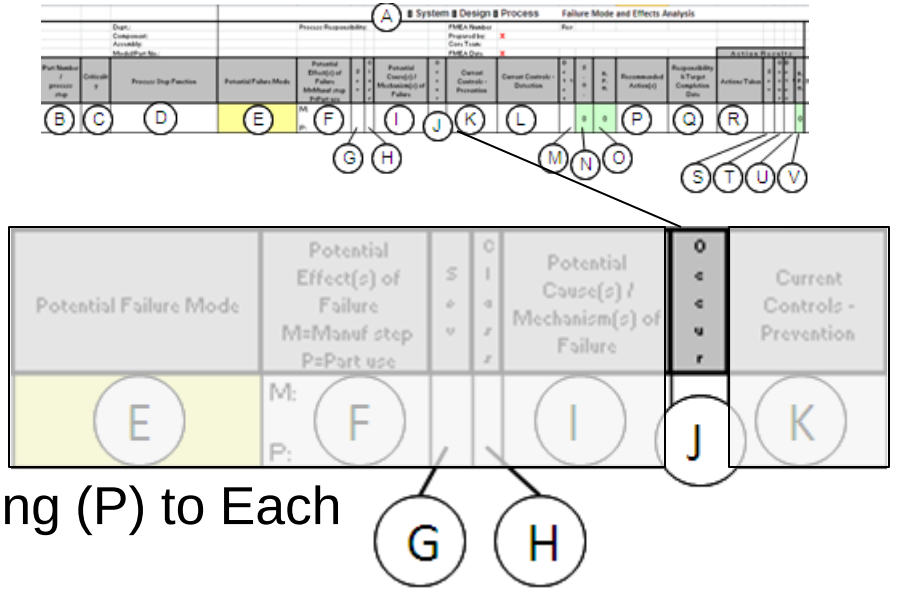
- Describe Causes in Specific Terms, Not Ambiguous Phrases (E.g. Use “Operator Fails to Tighten Fixture”, Not “Operator Error”)

- For DFMEA: Design Weaknesses
- For PFMEA: Describe in Terms of Something Correctable or Controllable

FMEA

Performing a ***FMEA***

Phase II: Step J



Design and Process FMEA

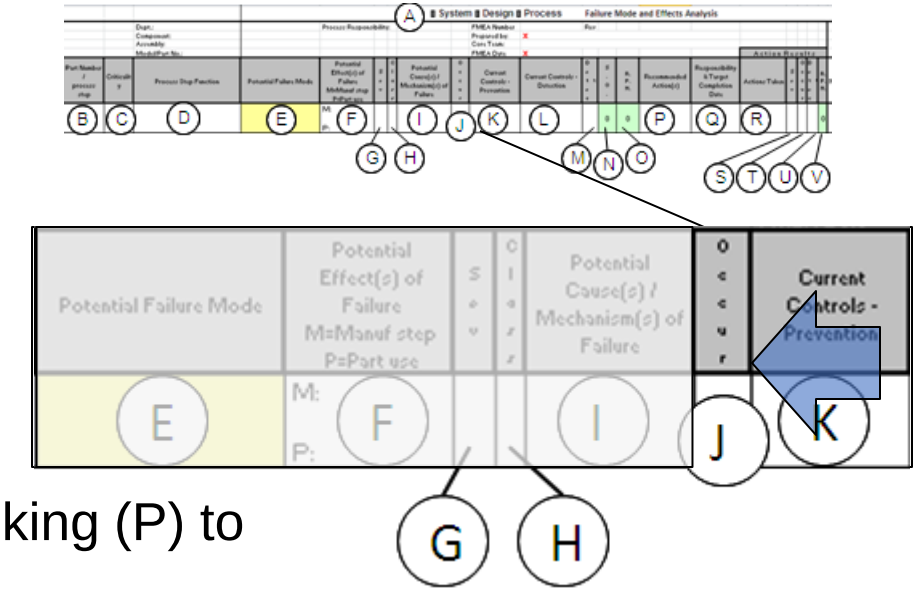
Step J: Assign an Occurrence Ranking (P) to Each Cause

- Assign Rank on Likelihood of the Cause Occurring
- Assign Rank on Likelihood of the PFM Occurring if the Cause Occurs
- Ranking Relative within Scope of FMEA
  - Consistency is Vital

FMEA

Performing a ***FMEA***

Phase II: Step J



Design and Process FMEA

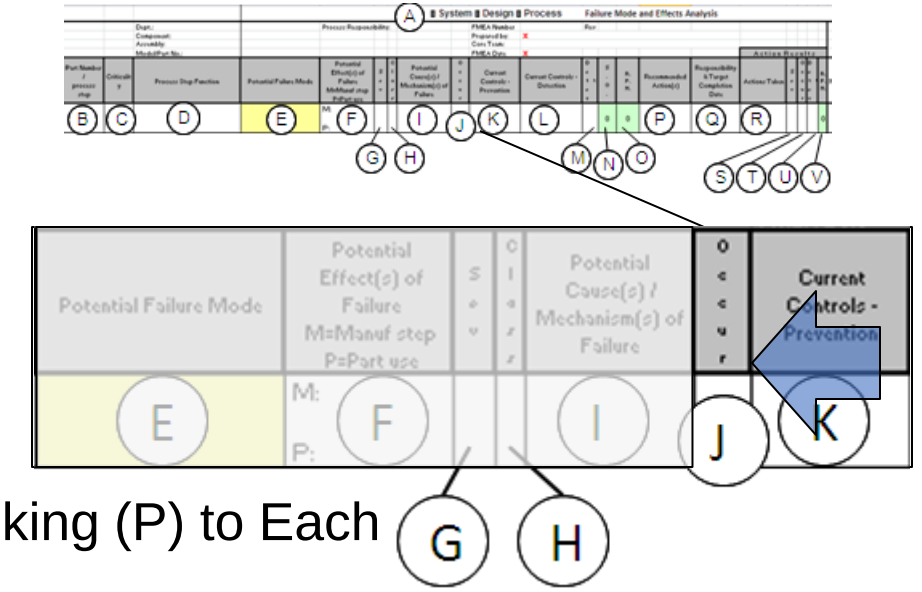
Step J: Assign an Occurrence Ranking (P) to Each Cause

- Consider Prevention Controls When Assigning Rank
- Occurrence Ranking Can Only Be Reduced Through Preventing or Controlling the Causes / Mechanisms of the PFM

FMEA

Performing a ***FMEA***

Phase II: Step J



Design and Process FMEA

Step J: Assign an Occurrence Ranking (P) to Each Cause

- Questions to Ask
  - What is the service history/field experience with similar components/process, subsystems, systems?
  - How significant are changes from a previous level component, subsystem or system? **(Change Point Analysis)**
  - Has the application changed?
  - What are the environmental changes?
  - Has a reliability analysis been used to estimate the expected comparable occurrence rank for the application?
  - What preventive controls been put in place?

FMEA

Performing a **FMEA**

Phase II: Step J

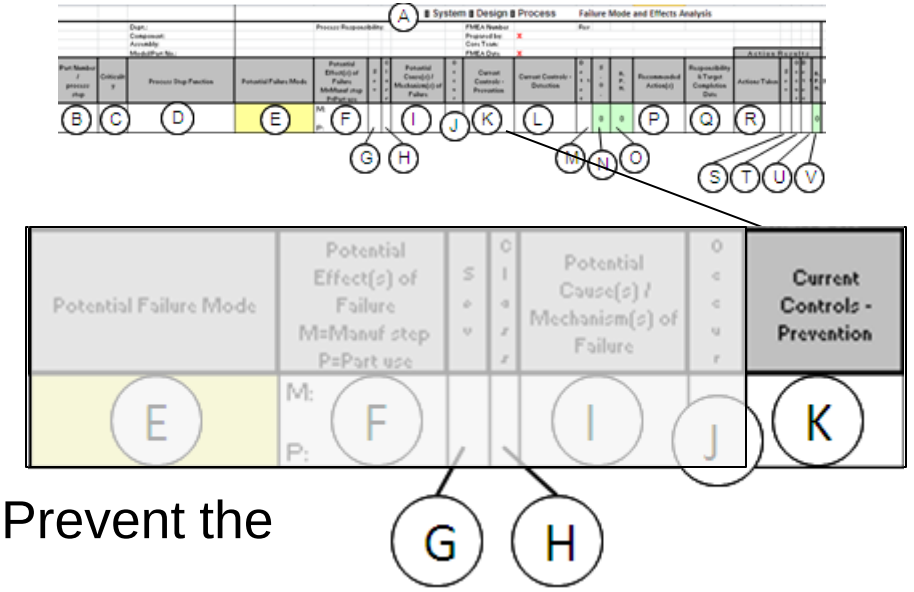
Design and Process FMEA

Rank	Occurrence
1	Remote: < 1 ppm
2	Very Low: < 1 in 20,000
3	Very Low: < 1 in 4,000
4	Moderate: < 1 in 1,000
5	Moderate: < 1 in 400
6	Moderate: < 1 in 80
7	High: < 1 in 40
8	High: < 1 in 20
9	Very High: < 1 in 8
10	Very High: < 1 in 2

FMEA

Performing a ***FMEA***

Phase II: Step k



Design and Process FMEA

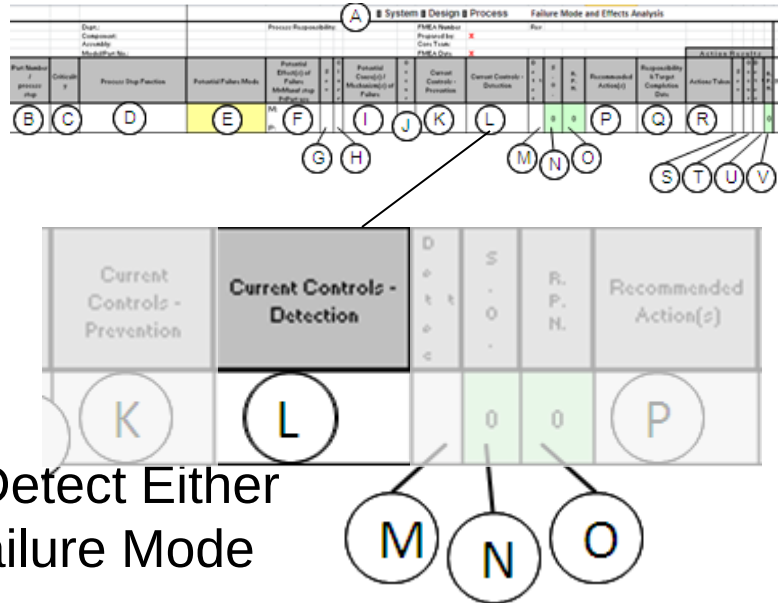
Step k: Identify Design Controls to Prevent the Cause (Prevention)

- Prevention Controls Can Prevent the Cause of the PFM or Reduce the Rate of Occurrence
- Prevention Controls Preferred Over Detection Controls

FMEA

Performing a ***FMEA***

Phase II: Step L



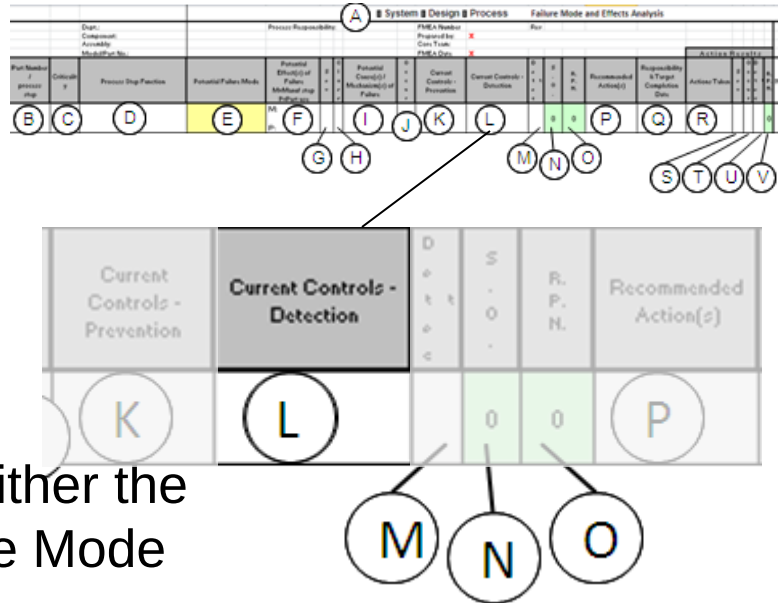
Design FMEA

Step L: Identify Design Controls to Detect Either the Cause of the Failure or the Failure Mode (Detection)

- Question: in the present design methodology, how are you detecting this failure, cause?

FMEA

Performing a ***FMEA***



Phase II: Step L

Process FMEA

Step L: Identify Controls to Detect Either the Cause of the Failure or the Failure Mode (Detection)

- For PFMEA: Detection May Occur at current operational step or Subsequent Operations

  If not detectable until later process steps, it may result in scrapping the part because it is no longer rework able

FMEA training

Performing a ***FMEA***

Phase II: Step K & L

Design and Process FMEA

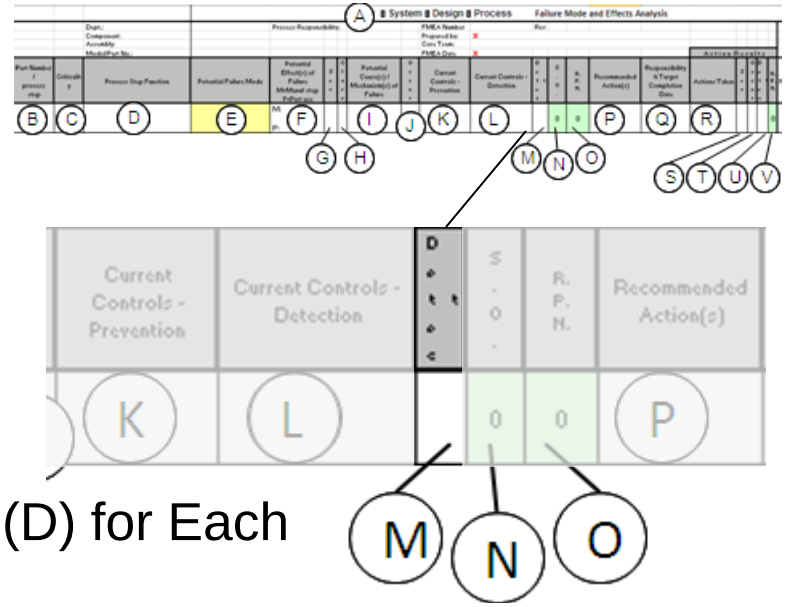
Step K and L: Prevention and Detection Design (or Process) Controls

Control	Category	Example
Prevention (Lower Cost)	DFA (Design for Assembly)	Print Specific, Packaging, Parts Can Not Fit Backward
	Supplier Controlled	Supplier Control Plan
	Process Step Sequence	Interdependent Sequence of Operations
Detection (Higher Cost)	Component Level Mistake Proofing	Fixtures, Tools, Safety Controls
	Manual Check-Over	SPC, Visual Checks, Weighing
	In-Process Verification (Subsystem Level Checks)	Destructive Testing, X-Ray, Humidity Check
	Functional Testing	Electrical Test, Helium Leak Test, Tensile Testing, Bend Tests
	Performance or Reliability Checks	Life Test

FMEA

Performing a ***FMEA***

Phase II: Step M



Design FMEA

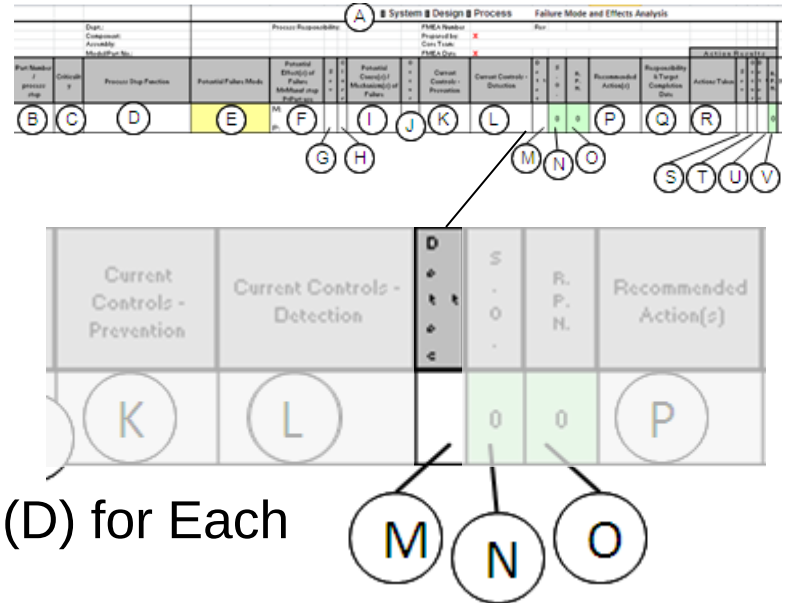
Step M: Assign a Detection Ranking (D) for Each Control

- Rank the Ability of the Design Control to Identify a Design Weakness or Cause Before Production Release
- Do Not Assume Detection Rank is Low Because Occurrence Rank is Low
  - Assess Ability of Design Controls to Detect Low Frequency Failure Modes
- Detection Ranking Can Only Be Reduced Through Improving Design Controls

FMEA

Performing a ***FMEA***

Phase II: Step M



Process FMEA

Step M: Assign a Detection Ranking (D) for Each Control

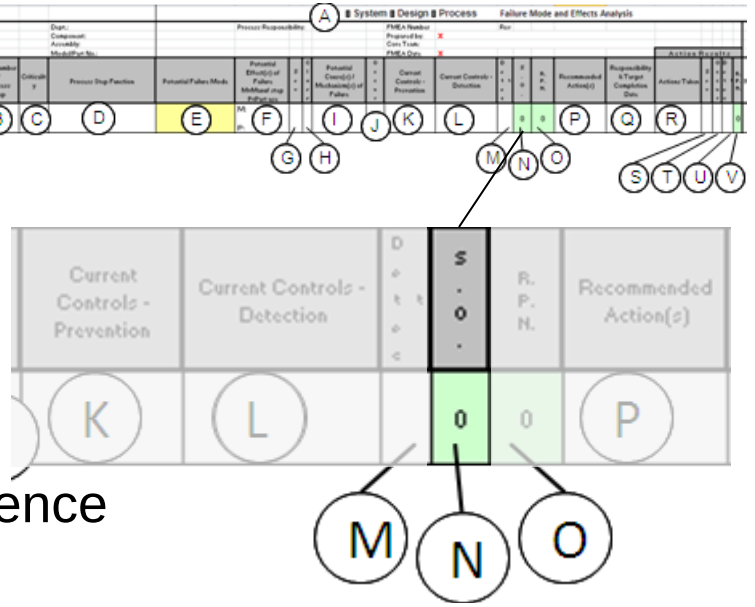
- Rank the Ability of the Process Control to Identify Parts with the Failure Mode and Prevent Them From Being Accepted / Moved to Next Process Step / Shipped

- Do Not Assume Detection Rank is Low Because Occurrence Rank is Low
  - Assess Ability of Process Controls to Detect Low Frequency Failure Modes

FMEA

Performing a ***FMEA***

Phase II: Step N



Design and Process FMEA

Step N: Assess the Severity x Occurrence number for necessary action

- Severity 10 always has to have an action
- SxO rankings above 60 should be considered actionable
- Detection Ranking may be low, but that doesn't excuse the item from action

FMEA

Performing a ***FMEA***

Phase II: Step J

Design FMEA

Rank	Detection
1-2	Design verification technique has a very high effectiveness in detecting this potential cause.
3-4	Design verification technique has a moderately high effectiveness in detecting this potential cause.
5-6	Design verification technique has a low to moderate effectiveness.
7-8	Design verification technique has a very low effectiveness in detecting this potential cause.
9-10	Design verification doesn't exist or is unproven or unreliable in detecting this potential cause.

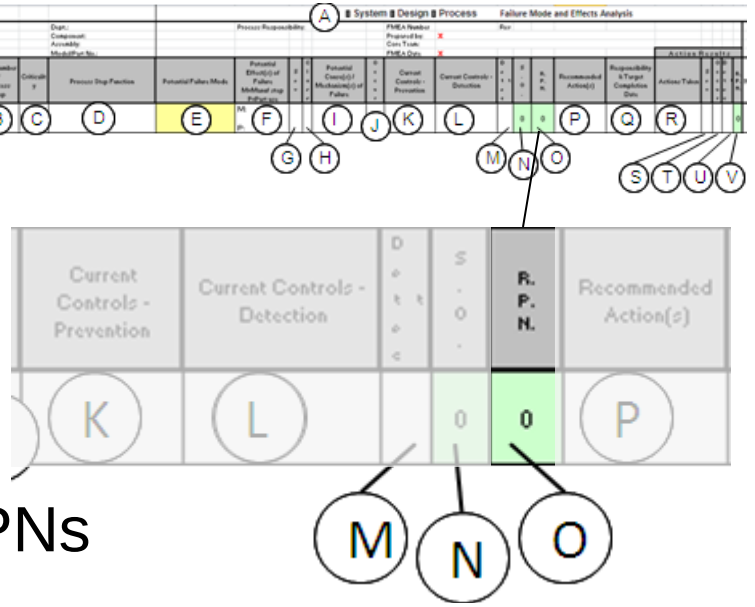
Process FMEA

Rank	Detection
1	Controls certain to detect / prevent defect.
2-3	Controls have a good chance of detecting / preventing defect.
4-5	Controls may prevent / detect defect.
6-7	Controls have a poor chance of detection / prevention of defect.
8-9	Controls are unlikely to detect / prevent defect.
10	Absolute certainty of non-detection.

FMEA

Performing a ***FMEA***

Phase II: Step K



Design and Process FMEA

Step K: Calculate and Rank RPNs

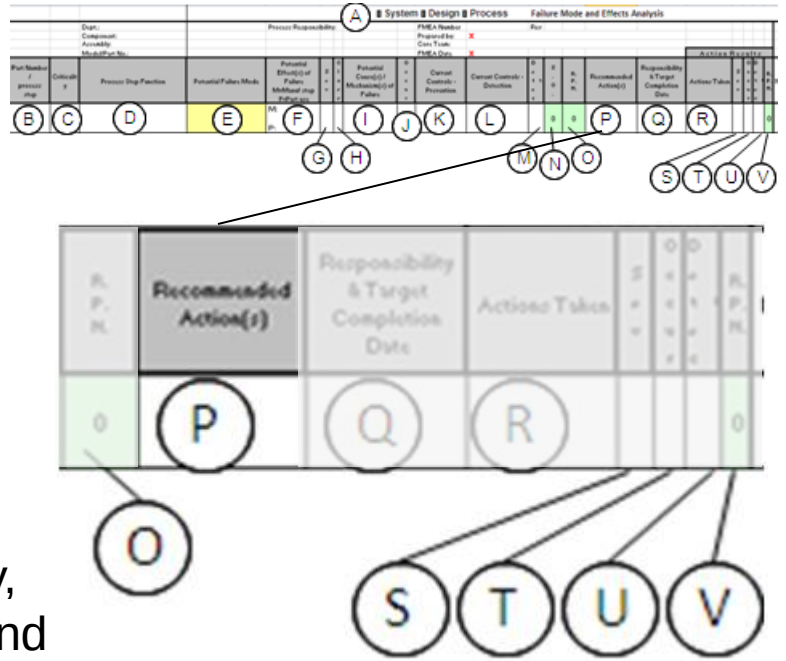
RPN = S x P x D

RPN threshold established at beginning of process

- Severity of 10 is always actionable
- RPN=100 is a typical threshold
- Under certain circumstances, 20/80 rule may be used

FMEA

Performing a **FMEA**



Phase II: Step P

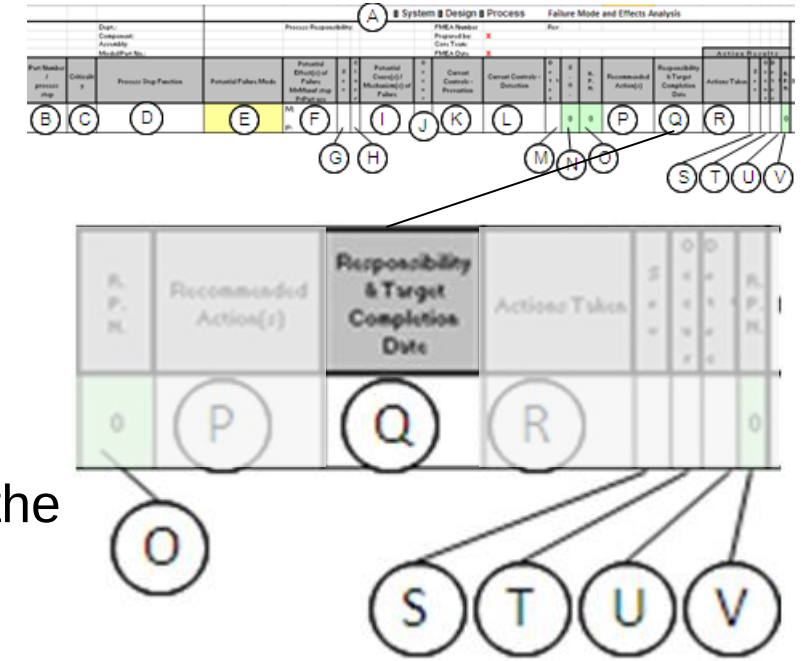
Design and Process FMEA

Step P: Develop the Recommended Actions. CAPA database Entry.

- Seek to First Reduce the Severity, Then the Occurrence (Prevent) and finally the Detection.
- Severity Changes Almost Always Require a Design and/or Process Revision. This Should Not be Neglected During the Exploration of the Recommended Action.
- The Recommended Action Doesn't Always Become the Action Taken.
- Recommended actions should be launched as soon as a high SxO or RPN is listed

FMEA

Performing a ***FMEA***



Phase II: Step Q

Design and Process FMEA

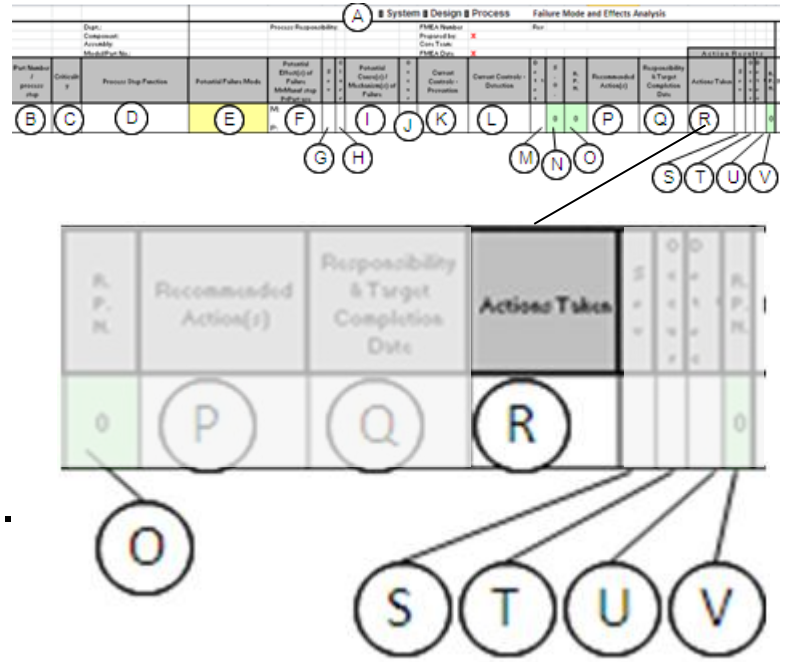
Step Q: Identify the Responsible Person, or the Department, and the Target Date for Completion.

- The Responsible Person Should be on the Team and May Need to Identify Who Will Actually Take the Action. There are also Resource Loading Considerations to be Dealt With.

- Target Dates are Typically Driven by the Project Timelines. Take into Consideration that the Completed Action Item is Required for the Project.

FMEA

Performing a ***FMEA***



Phase II: Step R

Design and Process FMEA

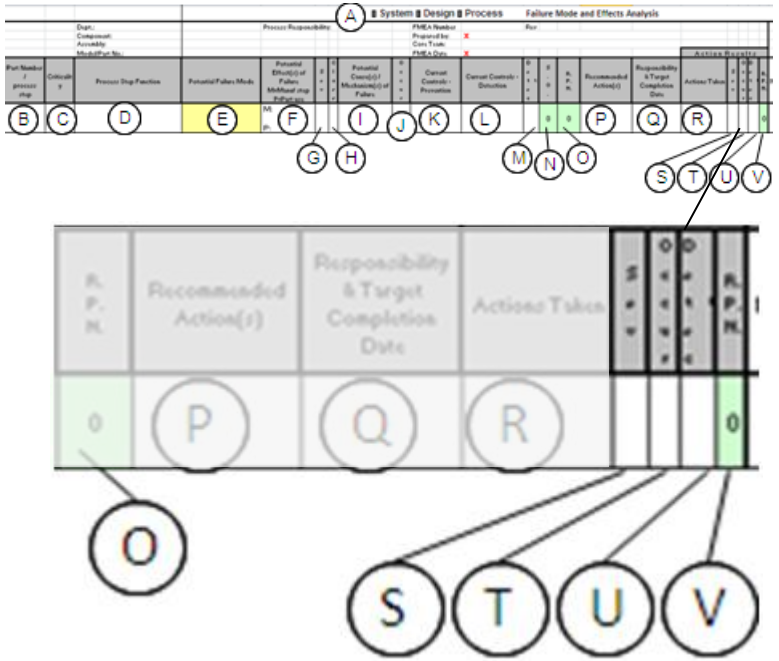
Step R: Enter the Actual Action that was Taken and the Effective Date. CAPA Database Entry

- A Concise Statement Should Describe the Action. Show the Linkage Back to the CAPA Database.

- If Related Documents are Involved, Include the References for Future Updates.

FMEA

Performing a ***FMEA***



Phase II: Step S,T,U,V

Design and Process FMEA

Step S,T,U: Calculate the new rankings

RPN = S x P x D

Step V: Assess the new RPN against the RPN threshold and determine if further action is required.

Common Mode Analysis

To avoid confusion it is necessary to distinguish this concept from that of common cause variation as applied to control charts. A common cause failure (CCF) occurs when two or more components fail at the same time as a result of a shared cause. Recognizing and mitigating common cause failure is a vital part of designing for reliability. These failures often are not exhibited from the standard fault tree analysis.

Common cause failures are either common event failures, where the cause is a single external event, or common mode failures, where two systems fail in the same way for the same reason. Common mode failures can occur at different times because of a design defect or a repeated external event.

Hazards Analysis

A hazard is a condition, event or circumstance that could lead to or contribute to an unplanned or undesirable event.

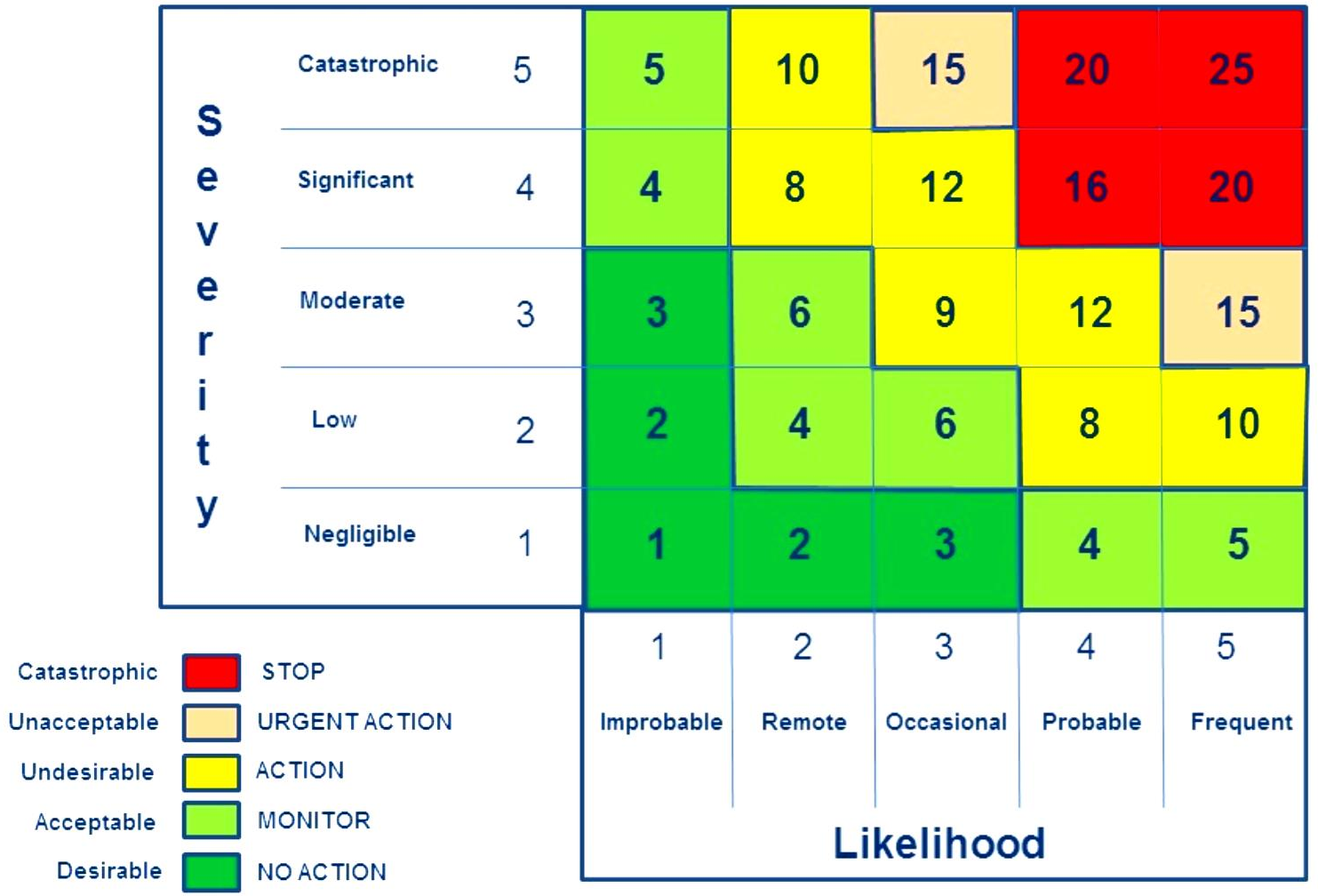
Most often used early in the development

Three fundamental questions are asked:

1. What might go wrong? The risk
2. What is the probability that it will go wrong? The likelihood
3. What are the consequences? The severity

As in the FMEA, the hazard is then the combination of the likelihood and the severity of the risk.

Hazards Analysis



Risk Matrix

	Importance	Risk types																					
		Technical			Scheduling				Safety		Financial			Regulatory				Supplier			Materials			Etc.
		A	B	C	A	B	C	D	A	B	A	B	C	A	B	C	D	A	B	C	A	B	C	
Product 1																							
Product 2																							
Product 3																							
Service 1																							
Service 2																							

Basic Reliability Terminology

- Availability
  - Definition: MTTR (mean time to resolve) is the average time it takes to fully resolve a failure. If the product is repairable , requires no Preventive Maintenance, and if repair can begin immediately when the failure occurs.

$$A = \frac{MTBF}{MTBF + MTTR}$$

Alternatively,

$$A = \frac{average\ uptime}{average\ uptime + average\ downtime}$$

System Safety

Identification of Safety Hazards

Reliability practitioners must be diligent in the discovery of all possible ways that any failure, combination of failures, or other combinations of circumstances could present a safety hazard to personnel.

Risk Analysis

The standard analysis techniques

- Failure Mode and Effects Analysis (FMEA),
- Failure Mode, Effects, and Criticality Analysis (FMECA),
- Production Reliability Acceptance Test (PRAT),
- Fault Tree Analysis (FTA),
- Success Tree Analysis (STA),
- Failure Reporting, Analysis, and Corrective Action System (FRACAS)

System Safety

Corrective and Preventive Action

Actions should be employed for any risk analysis technique in general, and in the case of Safety Hazards, there is an additional prioritization and urgency to ensure Safety of personnel. (includes manufacturing, assembling, testing, usage, foreseeable misuse and obsolescence for all involved and for society in general)

As Low As Reasonably Practically (ALARP)

In the U.K., the term “SFAIRP” is also commonly used, standing for “So Far As Is Reasonably Practicable.” It has the same essential meaning as ALARP, and is the term most commonly used in safety regulations, and for health and safety at work.

The risk is weighed against the sacrifice (cost) that is necessary to reduce the risk. The decision is weighted in favor of safety and health, because it must be shown that the sacrifice is hugely disproportionate to the safety and health benefits.

System Safety

Human Error and Mistake Proofing

Procedures for preventing/mitigating human error are variously called:

- Idiotproofing
- Mistake-proofing
- Poka-yoke
- Zero Quality Control (ZQC)

Human error tends to fall into the following categories:

- Misunderstanding
- Misidentification
- Inexperience
- Inattention
- Lack of standards

Mitigation

Phases include new design, continuous improvement and End Of Life

Strategies to minimize risk:

- Elimination by design
- Reduction by alternative method/material
- Implementation of protective measures (passwords, guards, visuals, etc.)
- Implementation of warning systems (alarms, lights, signage, etc.)
- Administrative controls (training, policies, etc.)
- Personal Protective Equipment (PPE)
- Obsolescence strategies
  - Point of view of the Producer
  - Point of view of the customer