Risk Management and Applications of System Safety

Vincent Ho

21 Sep 2008

Contents

- Introducing System Safety
- Risk Management Principles
- Risk vs Hazards
- Case Study on System Safety Application

What is System Safety?

HKARMS

System Safety is Not Merely…

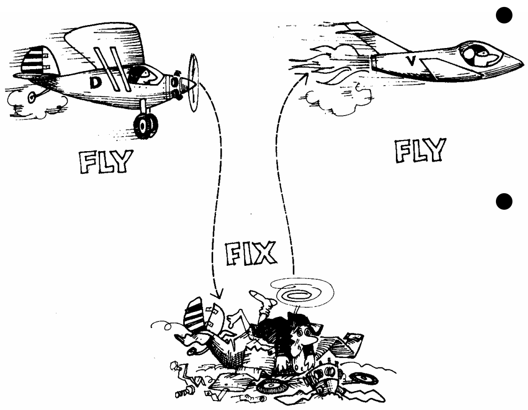
- A hazard logging system;
- A set of quantitative Reliability, Availability, Maintainability, and Safety criteria for system design;
- An application of FMEA, PHA or QRA;
- Requirements for contractors; or
- A set of documentation to satisfy approval authority

System Safety ≠ Systems Safety

System Safety is….

- The application of engineering and management principles, criteria, and techniques to optimise Safety within the constraints of operational effectiveness, time, and cost throughout all phases of the System life cycle
- Primarily a management tool that applies special technical and managerial skills to the systematic, forward-looking identification and control of hazards throughout the life cycle of a project, program, or activity
- Addressing safety at a system level
  "A system is a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software"

History of System Safety



- The System Safety Program grew out of the aerospace and military programs to improve safety
- The proactive system-level approach replaced the fly-fix-fly approach

- **1962: System Safety Engineering for the Development of Air Force Ballistic Missiles**
- **1969: MIL-STD-882, System Safety Program Requirements**

History of System Safety

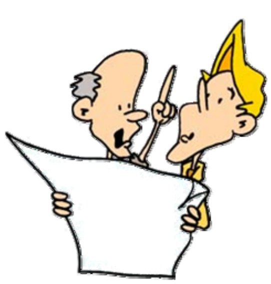
- The aviation industry significantly improved its safety records in the 60s and 70s
- "Today, there are more people killed by donkeys annually than by air crashes"
- Nowadays, System Safety has been commonly applied in major industries such as military/ defense, chemical processing, aerospace, power generation and distribution, transportation, etc.



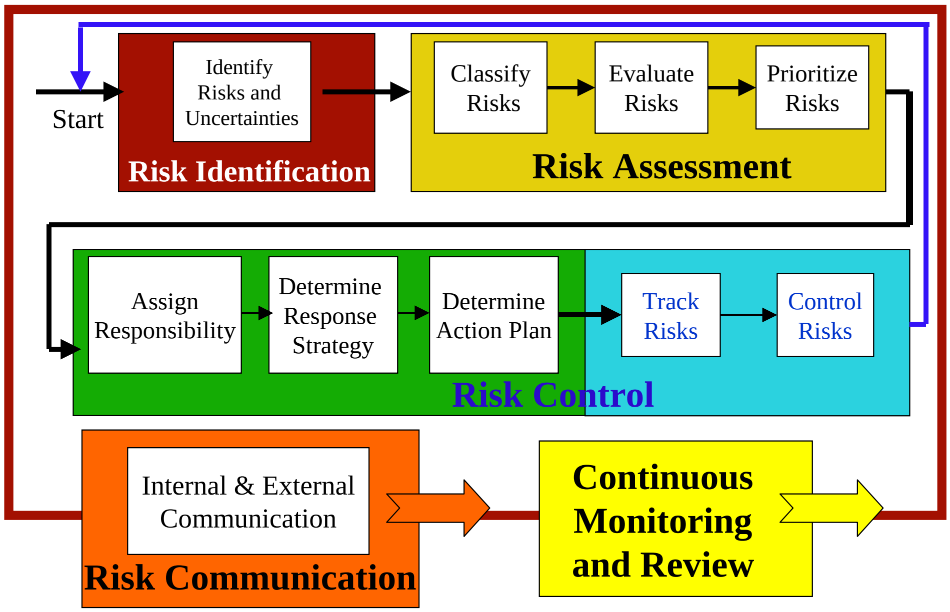

Objective of System Safety

- To achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management

MIL-STD-882D, Department of Defense, USA




Key Steps in a Risk Management Programme



Risk Management Principles

HKARMS

Risk Management

- Risk Management is a term given to a set of practices that lead to minimizing possible harm to individuals
- While it may not be possible to totally protect individuals, a risk management system seeks to identify factors that may increase those risks and actively promote practices that will keep risk as low as reasonably practicable

HKARMS

Risk Management Principles

- Prevention of serious incidents is the highest priority
- Safe and accessible environments are everyone's responsibility
- Continuous communication, accurate reporting, consistent analysis of information, and development of sound, person-centered strategies are essential to prevent serious incidents

HKARMS

Risk Management Principles

- Staff are competent to respond to, report and document incidents in a timely and accurate manner
- Individuals have the right to a quality of life that is free of abuse, neglect, and exploitation
- Risk management systems should emphasize staff involvement as integral to providing safe environments
- Quality of life starts with those who work most closely with persons receiving services and supports

HKARMS

Elements of Effective Risk Management

- Training of all involved in supporting individuals with developmental disabilities in the risk management process
- Individual risk assessment, evaluation, and planning
- A well-defined process for reporting incidents that is timely, complete, and accurate
- Immediate follow up and intervention to ensure health and safety and to mitigate future risk

Elements of Effective Risk Management

- Regular review and analysis of incidents by a risk management, assessment and planning committee
- Trending of data to detect patterns and facilitate development of risk mitigation strategies
- Proactive measures to prevent or minimize the likelihood of further incidents

Purpose of Risk Management

- To address liability issues
  - Have you done enough to avoid the accident?
- To optimise resources ($) by balancing cost, risks and benefit
- To rank order minor risks from major
- To compare different options
- To provide information for decisions

HKARMS

Decision Making

Decision Options

- Not to continue with the activity
- Conduct more detailed analysis for further information
- Treat and Control Risks
- Accept risk without further action (To do nothing!!)

Criteria Options

- Regulated limits
- Regulatory guidance
- Company goals
- Good will
- Social responsibility
- Financial Costs
- Risk
  - Risk-based decision
  - Risk-informed decision

HKARMS

Principles of Risk Control

- Risk Elimination
- Risk Avoidance
- Risk Transfer
- Risk Reduction
- Risk Absorption

Chance only favors the prepared mind.

Louis Pasteur

Recognizing Risk

- You have to recognize risk before you can understand risk
- You have to understand risk before you can assess it
- You have to assess risk before you can manage or control it

Defining Risk

HKARMS

Two Key Questions

- How safe is safe?
- What level and how much can you afford safety?

- To answer these questions, we must be able to quantify safety
- However, safety cannot be directly measured

HKARMS

Definitions of Risk

$$\text{Risk} = \text{Likelihood} \times \text{Consequence}$$

- Classical, but most misleading. More useful in hazard analyses

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}}$$

- Risk is never zero by increasing level of safeguards, as long as hazard is present

$$\text{Risk} = \text{Uncertainty} \times \text{Damage}$$

- Without uncertainty or damage, there is no risk

HKARMS

Quantitative Definition of Risk

- In general, risk is used to answer:
  - What can go wrong?
  - How likely is it that this will happen?
  - If it happens, what are the consequences?
  - What are the uncertainties?
- Thus, risk can be thought to be consisting of four elements:
  - Scenarios
  - Likelihood
  - Consequence
  - Uncertainties

HKARMS

Quantitative Definition of Risk

Scenario	Likelihood	Consequence
s_1	L_1	C_1
s_2	L_2	C_2
s_3	L_3	C_3
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
s_N	L_N	C_N

- Risk = $\{<S_i, L_i, C_i>\}$
- For each S_i, $Risk_i = L_i \times C_i$
- Total risk of the system is $R = \Sigma_i L_i \times C_i$

Uncertainties

- Uncertainties are measured by level of belief
- In general, there are three types of uncertainties associated with a risk model:
  - Stochastic uncertainties
  - Modelling uncertainties
  - Parameter uncertainties
- Without an explicit consideration of uncertainties, the result of a risk analysis can be meaningless
- Probability is used as the measurement scale
  - Strictly speaking, $A+A \neq 2xA$

Sources of Uncertainty

- No access to the whole truth
- No categorical answer
- Incompleteness
  - The qualification problem - impossible to explicitly enumerate all conditions
- Incorrectness of information about conditions
- The rational decision depends on both the relative importance of various goals and the likelihood of its being achieved

HKARMS

Probability vs Frequency

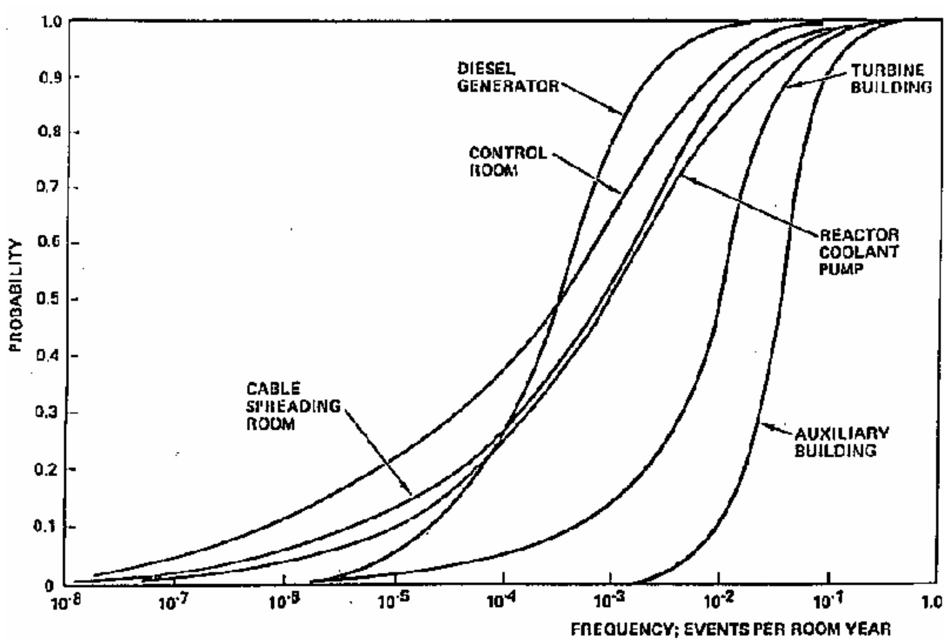
- Frequency is a measure of the rate of occurrence. E.g., failure rate of a pump is 6.2×10^{-3}/hr
- Probability is a measure of the level of belief, a fraction, or failure per demand. It is dimensionless
  - P=0 for false event
  - P=1 for sure event or event that has occurred
- Probability can be used to measure uncertainties in frequency' e.g., the failure rate of the pump is

Frequency	Probability
1.0×10^{-4}/hr	0.2
2.0×10^{-3}/hr	0.5
3.2×10^{-3}/hr	0.2
4.5×10^{-2}/hr	0.1

with a mean of 6.2×10^{-3}/hr

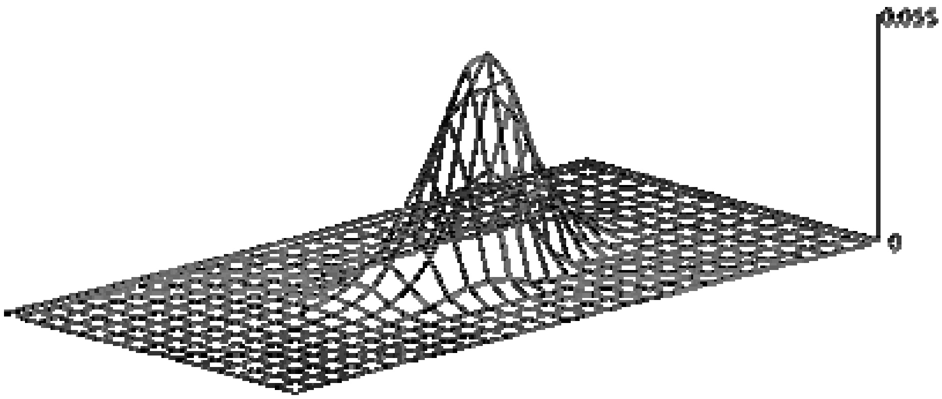
HKARMS

Probability Curves for Frequency



HKARMS

Probability Curves for Frequency



Risk vs Hazard

Risk vs Hazard

RISK	HAZARD
↓	↓
What might go wrong	Sources of harm
How it might happen	Causing a damage

Risk vs Hazard

- Risk has been defined in various ways in different industries, and is often misunderstood and misapplied
- Risk is relative
- To characterise risk, we must have:
  - A hazard-source of danger
  - An initiating event that activates the danger
  - A target (risk receptor)
  - A transfer mechanism to expose the target to the dangerous situation

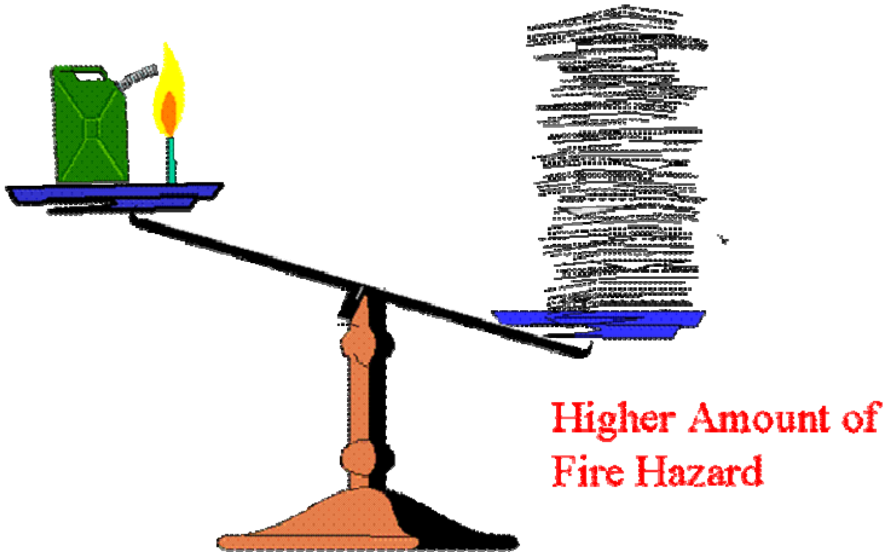
HKARMS

Risk vs Hazard

- Hazard is a source of danger, or the presence of a condition or a situation, that has the potential of resulting in undesirable consequences
- Hazard can be measured by absolute terms; e.g., weight, volume
- Hazard is a relative term
  - Fire is a hazard to life
  - Gasoline is a fire hazard

HKARMS

The Amount of Hazard does not Necessarily Indicate the Risk Level

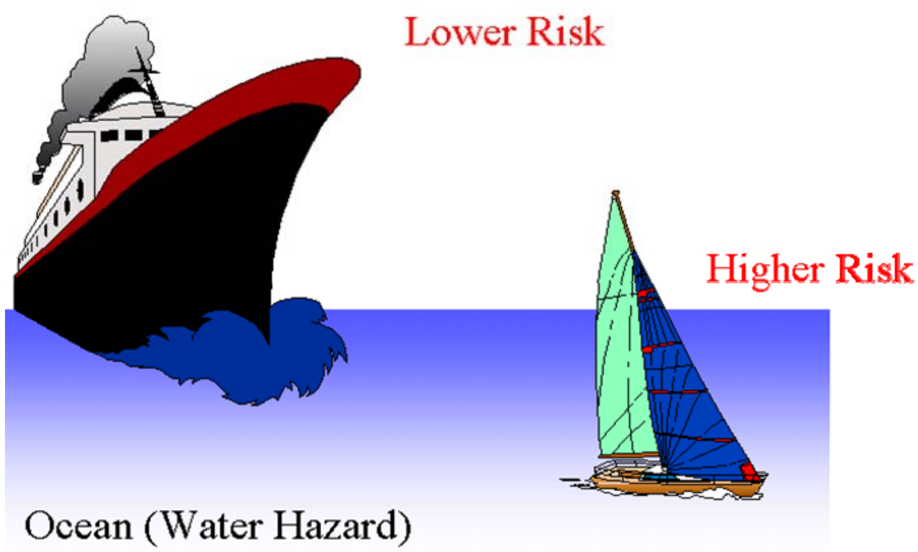


HKARMS

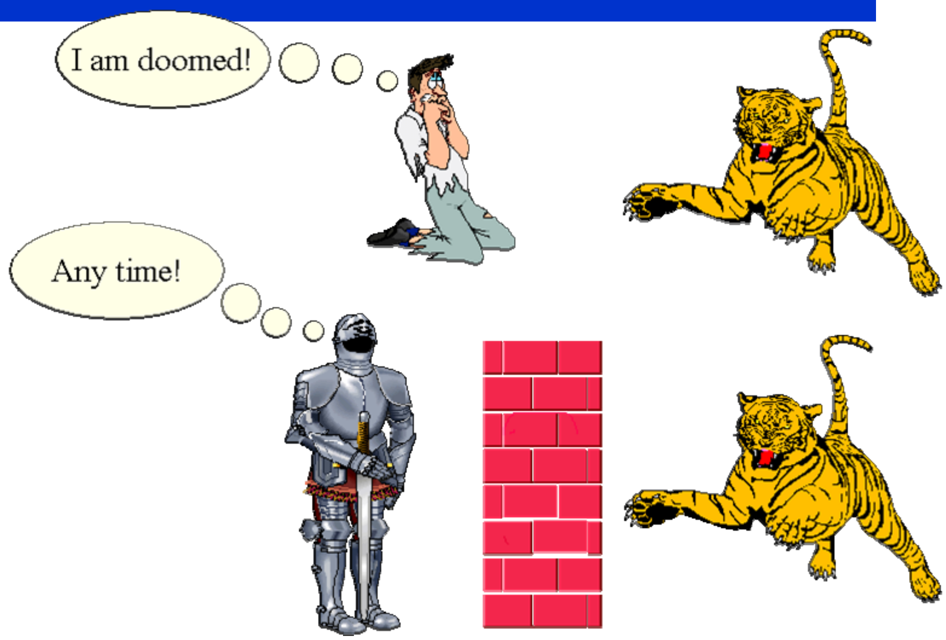
The Totality of a Situation is a Better Indicator of the Risk Level

HKARMS

Same Hazard might Cause Different Risk Levels to Different Targets



Same Hazard may Impose Different Risks due to Different Safeguards



HKARMS

Example of Hazards

- A foreign material, e.g., methane gas in confined space
- A situation or a condition, e.g., loose slope
- A design compromise or inadequacy, e.g., a weak structure or a lack of safety measures
- A failure of a component or a system, e.g., lifting apparatus failure
- A latent failure of a component or a system, e.g., gas detector fails to detect gas at dangerous level

Typical Hazard Analysis Tools

- Open ended questions with brainstorming - what if
- Check lists, Hazard lists
- Preliminary hazard analysis
- Failure Mode and Effect Analysis
- Hazop
- Fault Trees

Hazard Evaluation

- No standard way, the complexity of the evaluation depends on the application and industry
- Typically use MIL-STD-882 style look up table to characterise likelihood and consequence
  - Very popular, quick and easy
  - Has become “the” method in hazard evaluation due to lack of expertise and resources
- Look up tables → risk matrices

Contract No: System: Subsystem:				Hazard Analysis Work Sheet						Prepared by: Reviewed by: Authorised by:							Date: Date: Date:		
Ref No.	Hazard Scenario Description/ Consequence	Op. Mode	Existing Safeguard/ Control Measure	Risk Impact				Proposed Mitigation Measures/Control	Residual Impact				Comment/ Resolution	Status	Responsibility	Days Remained Open			
				L	C	R	G		L	C	R	G							

People often mistakenly think that it is THE" only way to do hazard or risk analysis… NOT

Worksheet Methods

- The most popular safety analysis approach is the risk-ranking method using worksheets to define hazard scenarios
- Each record (row) in the worksheet describes an independent scenario
- The approach uses discrete risk-ranking matrices to character likelihood, consequence and risk class

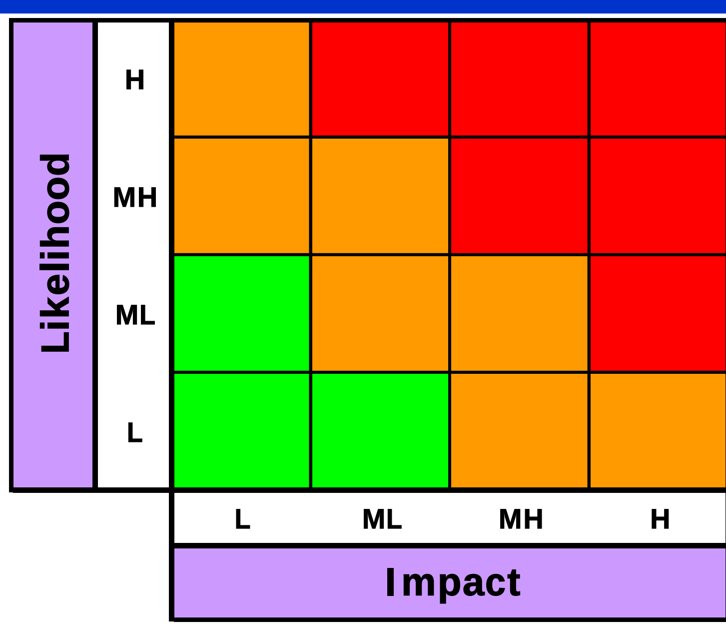
Strictly speaking, a worksheet type analysis is a Hazard Analysis, not a Risk Analysis

Using Risk Matrix

- Rank the safety risk using function of likelihood and consequence classes in the form of look up tables
- Also known as the Mil-Std-882 approach
- Unique combination of likelihood and consequence gives a risk class
- For qualitative screening purposes
- Rank-ordering hazard/risk scenarios

THERE IS NO STANDARD RISK MATRIX

Defining 'Risk Appetite'



Examples of Likelihood Scales

Scale	Likelihood
High (H)	Greater than once per day
Medium High (MH)	Greater than once per week
Medium Low (ML)	Greater than once per month
Low (L)	Greater than once per year

Railway Operations Managers

Board of a Battery Manufacturer

Scale	Likelihood
High (H)	Once a month
Medium High (MH)	Once a year
Medium Low (ML)	Once every five years
Low (L)	Once every twenty years

Examples of Impact Scales

Scale	Impact
High (H)	Partial line closure (or worse)
Medium High (MH)	Station closure
Medium Low (ML)	Journey delay > 2 mins
Low (L)	Journey delay < 2 mins

Railway Operations Managers

Board of a Battery Manufacturer

Scale	Impact
High (H)	Threatens business survival
Medium High (MH)	Long term damage to business
Medium Low (ML)	Short term damage to business
Low (L)	Trivial

HKARMS

Typical Risk Matrix

Likelihood \ Consequence	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain A	S	S	H	H	H
Likely B	M	S	S	H	H
Moderate C	L	M	S	H	H
Unlikely D	L	L	M	S	H
Rare E	L	L	M	S	S

H = High risk detailed research and management planning required at senior levels
S = Significant risk senior management attention needed
M = Moderate risk management responsibility must be specified
L = Low risk : manage by routine procedures

HKARMS

Example of Risk Matrices

Frequency Class	Consequence Class: R – Service-Related	C1 – Trivial	C2 – Minor	C3 – Serious	C4 – Critical	C5 – Disastrous
F1 – Frequent (>10/yr)	R	B	A	A	A	A
F2 – Common (1/yr to 10/yr)	R	B	B	A	A	A
F3 – Likely (0.1/yr to 1/yr)	R	C	B	A	A	A
F4 – Rare (0.01/yr to 0.1/yr)	R	C	C	B	A	A
F5 – Unlikely (10^{-3}/yr to 0.01/yr)	R	D	C	C	B	A
F6 – Improbable (10^{-4}/yr to 10^{-3}/yr)	R	D	D	C	C	B
F7 – Incredible (<10^{-4}/yr)	R	D	D	D	C	C

Risk Class	Description
A	**High Risk** – Risk control measures should be implemented to mitigate the risk to a level that is ALARP with a top priority.
B	**Medium Risk** – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP within a reasonable time.
C	**Low Risk** – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP with a low priority.
D	**Negligible Risk** – Risk is considered acceptable; no additional risk control action is normally required. Cost-effective risk control measures may be implemented to further mitigate the risk with the lowest priority.

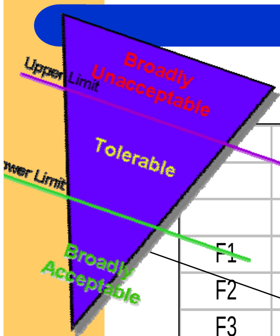
Another Example of Risk Matrix

			CONSEQUENCE						
			7	6	5	4	3	2	1
			Trivial	Negligible	Marginal	Serious	Critical	Catastrophic	Disastrous
Staff/Contractor Safety	Fatality						<5	5 or more	
	Major Injury					<5	5 or more		
	Minor Injury	with ≥ 3 days sick leave			<5	5 or more			
		with < 3 days sick leave		<5	5 or more				
Passenger/Public Safety	Fatality						<5	5-50	51-500
	Major Injury					<5	5-50	51-500	501 - 5000
	Minor Injury				<5	5-50	51-500	501 - 5000	>5000
Service	System Disruption				<20 min	1 hour	1 day	1 week	1 month
	Line Disruption			20-60min	few hours	1 day	1 week	1 month	few months
	Station Disruption		<20min	few hours	1 day	1 week	1 month	few months	1 year
FREQUENCY	A	Few times per week or more	≥ 100 /year	R3	R1	R1	R1	R1	R1	R1
	B	Few times per month	≥ 10 - <100 /year	R4	R2	R1	R1	R1	R1	R1
	C	Few times per year	≥ 1 - <10 /year	R4	R2	R2	R1	R1	R1	R1
	D	Few times in 10 years	≥ 0.1 - <1 /year	R4	R3	R2	R1	R1	R1	R1
	E	Once since operation	≥ 1E-2 - <1E-1 /year	R4	R3	R3	R2	R1	R1	R1
	F	Unlikely to occur	≥ 1E-3 - <1E-2 /year	R4	R4	R3	R3	R2	R1	R1
	G	Very unlikely to occur	≥ 1E-4 - <1E-3 /year	R4	R4	R4	R3	R3	R2	R1
	H	Remote	≥ 1E-5 - <1E-4 /year	R4	R4	R4	R4	R3	R3	R2
	I	Improbable	≥ 1E-6 - <1E-5 /year	R4	R4	R4	R4	R4	R3	R3
	J	Incredible	< 1E-6 /year	R4	R4	R4	R4	R4	R4	R3

Risk Matrix Can Also be Simple

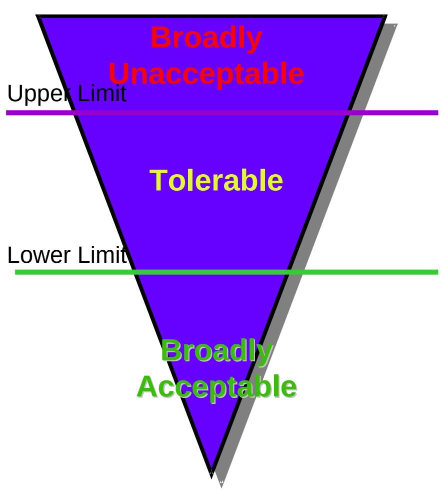
Risk Level	Description
High Risk	**The hazard may cause fatal or multiple serious injuries, for all ranges of frequency**
Medium Risk	**The hazard may cause single serious injuries, and the likelihood of having these kinds of injuries is quite probable**
Low Risk	**Other risk which is neither high nor medium**

Risk Matrix Should Actually be Designed by Quantitative Input



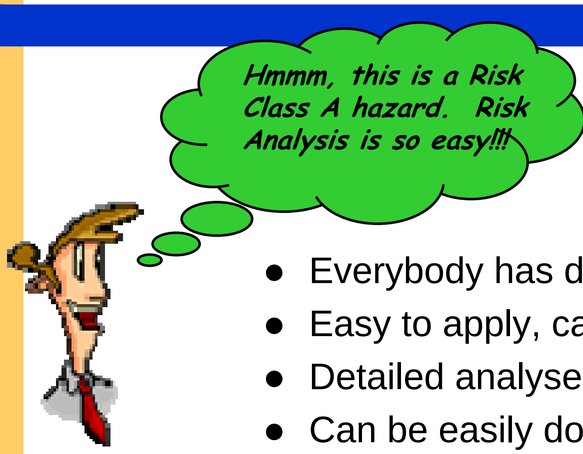
		0	0.001	0.01	0.1	1	10	20
		S1	S2	S3	S4	S5	S6	S7
	G. Mean	0.000	0.003	0.03	0.32	3.16	14.14	44.72
F1	31.62	1.00E-02	0.10	1.00	10.12	99.93	447.15	1414.21
F2	3.16	1.00E-03	1.00E-02	0.10	1.01	9.99	44.71	141.42
F3	0.32	1.00E-04	1.00E-03	1.00E-02	0.10	1.00	4.47	14.14
F4	3.16E-02	1.00E-05	1.00E-04	1.00E-03	1.01E-02	0.10	0.45	1.41
F5	3.16E-03	1.00E-06	1.00E-05	1.00E-04	1.01E-03	9.99E-03	0.04	0.14
F6	3.16E-04	1.00E-07	1.00E-06	1.00E-05	1.01E-04	9.99E-04	4.47E-03	0.014
F7	0.00	1.00E-08	1.00E-07	1.00E-06	1.01E-05	9.99E-05	4.47E-04	1.41E-03

ALARP: As Low As Reasonably Practicable



- Commonly adopted in UK and related systems
- Broadly distinguish risks into 3 regions
- If risk falls into Tolerable (ALARP) region, risk reduction is introduced unless the cost is grossly disproportional to the improvement gained
- Many gray areas

Advantages of Worksheet Methods

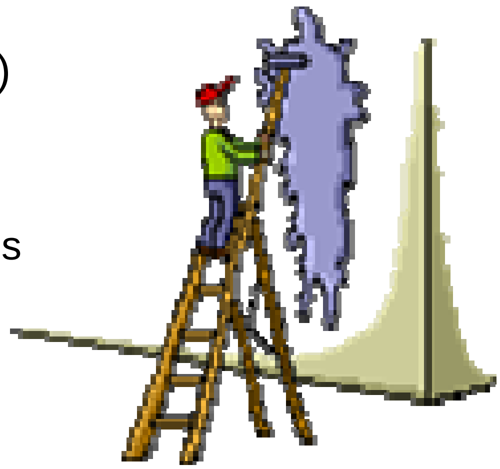


- Everybody has done one before
- Easy to apply, can be used by non-experts
- Detailed analyses not required
- Can be easily done in spreadsheet such as Excel
- Useful in evaluating a large number of alternatives with obvious differential risks

Using Risk Matrices: How to Beat the System

Manage the Risk of Painting?

- QRA? No.
- Hazard analysis (JHA?)
  - Identify hazard
  - Analyse and evaluate
  - Recommend measures
  - Monitor and review



Using Worksheet and Risk Matrix

Hazard	Consequence	Prob	Severity	Risk Class
Struck by falling object	Severe head injury	Med	High	I

Severity / Probability	Low	Med	High
Low	IV	III	II
Medium	III	II	I
High	II	I	I

I = High Risk… IV=Negligible Risk, no further action

HKARMS

Using Worksheet and Risk Matrix

Hazard	Consequence	Prob	Severity	Risk Class
Struck by falling paint can in Room 230A	Minor head injury	Low	Low	IV

Severity / Probability	Low	Med	High
Low	IV	III	II
Medium	III	II	I
High	II	I	I

- Break down high risk item into small items
- Create a pile of papers, etc.
- No additional work is needed!

HKARMS

Another Example of Mis-Using a Risk-Ranking Worksheet

Hazard	Consequence	Prob	Severity	Risk Class
Pump Room fire	Both pumps fail	Med	High	A

Severity / Probability	Low	Med	High
Low	D	C	B
Medium	C	B	A
High	B	A	A

- **Pump Room fire is not a rare event**
- **Losing both pumps will loss cooling**

Example of Mis-Using a Risk-Ranking Worksheet

Hazard	Consequence	Prob	Severity	Risk Class
Pump A on fire	Pump A damaged	Low	Med	C

Severity / Probability	Low	Med	High
Low	D	C	B
Medium	C	B	A
High	B	A	A

- **A high risk location can be easily broken down into components many sub-items (rows) with a lower risk for each sub-item**

Typical Mistakes in using Worksheet/ Risk Matrices

- Mix up risk matrices, if use L/C/R must show all 3 values
- Show scoring matrices but did not show scores
- Mix up potential cause and hazard scenarios
- Scenario description not concise
- Did not show residual risk
- Miss key hazards (e.g., spatial separation)
- Provide PPE is not the best bet

HKARMS

Disadvantages of Worksheet Methods

- Anyone can be an instant expert, results can be inconsistent between users
- Difficult to verify assumptions and results
- Cannot evaluate complex situation
- Difficult to identify common mode failures, system interactions, cascaded failures, etc.
- Cannot add up risks
- **Cannot compare alternatives in same risk class**
- **Cannot yield the total risk of a system**

HKARMS

Problems with Most Identification Tools

- What if thinking is difficult for some
- People do not perceive normal work conditions to be a hazard
- People not trained in safety may not know what is a hazard
- People are reluctant to spend time and effort at the planning stage
- Copying other people's hazard list is easy... And often meaningless

Case Study:

Verifying System Safety Acceptance of Guaranteed Emergency Brake Rate (GEBR) of a Light Rail System

HKARMS

Railway 101

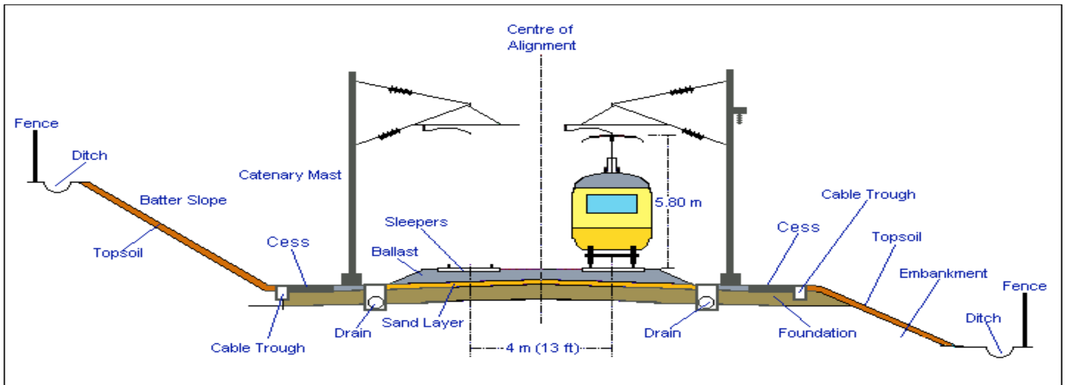
- Locomotives, EMU (not edible), diesel multiple units, heavy ra … in, … (no steer
- Flags, si … ATP, ATO, AT

showing names of principal parts of construction

HKARMS

Railway 101

- Locomotives, EMU (not edible), diesel multiple units, heavy rail, light rail, metro, subway, rolling stock, train, … (no steering wheel!)



Cross Section of Double Track Railway Alignment showing names of principal parts of construction

HKARMS

Rail Transit Operations

- Line-of-Sight
- Aspect Signaling (Colour Flags, Lights)
- Speed Codes
- Cab Signalling
- Automatic Train Protection (ATP)
- Automatic Train Control (ATO)
- Automatic Train Control (ATC)
- Manned vs Driverless System

HKARMS

Re-Signalling of a LRV system in California

- Background
  - Established (ageing) Light Rail Transit System
  - Part tunnel, part surface street
- System improvement
  - Purchase New Vehicles
  - Replace Train Control System
  - Improved throughput (reduce headway)
  - Improve safety

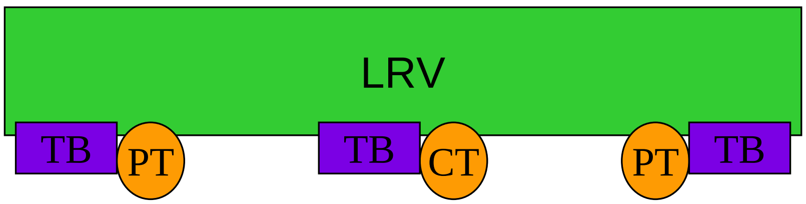
HKARMS

Guaranteed Emergency Brake Rate

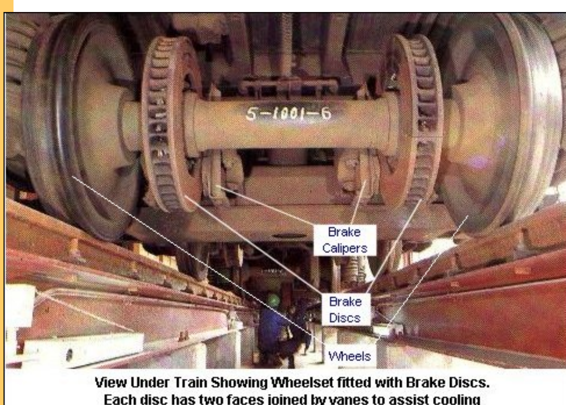
- Determine the minimum distance between trains; traditionally, 1.0 to 2.2 mphps
- Must be adequate to avoid collision within an acceptable safety margin
- Must be sufficiently high to minimize the time separation of trains (headway) but not too high too cause jerking
- limited by available rail adhesion (coefficient of friction)
  - Friction, rolling, sliding
  - Snow, wet leaves
  - Sand box

Braking System on these LRV

- Propulsion Brake (Dynamic Brake)
- Service Brake (Friction Brake)
- Emergency Brake (Friction Brake and Track Brake)
- On each coach of LRV (1 to 6+ units)
  - 3 sets of track brakes (TBs) (6 total)
  - 2 sets of power truck friction brakes (FBs) (4 total)
  - 1 set of center truck FBs (2 total)



Friction Brakes and Track Brakes



View Under Train Showing Wheelset fitted with Brake Discs.
Each disc has two faces joined by vanes to assist cooling

HKARMS

GEBR Verification Procedures

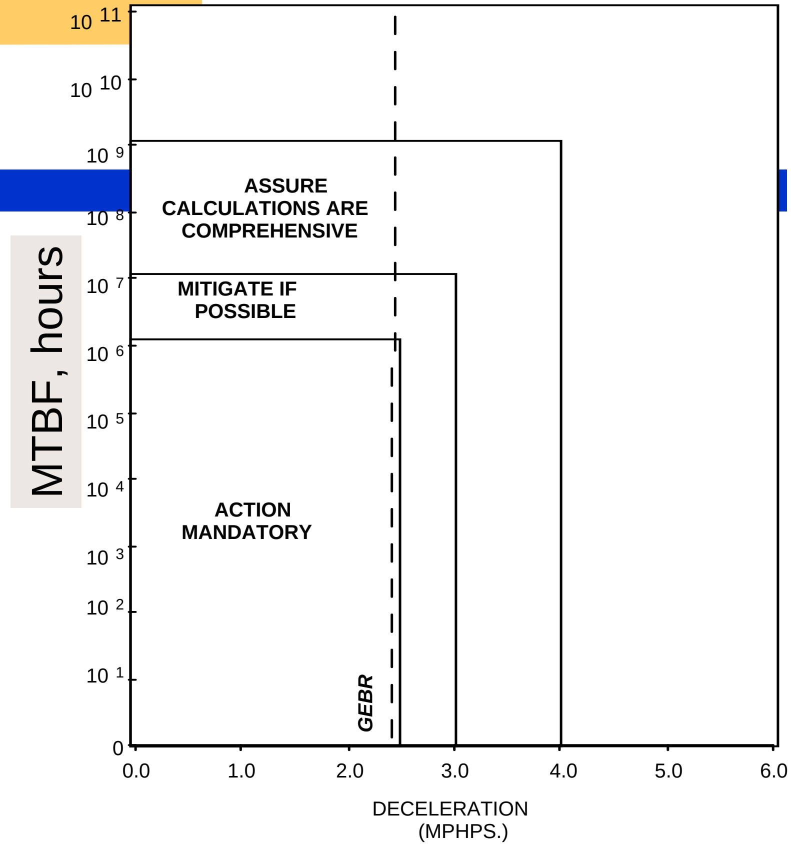
- Define Safety Margin
- Risk Identification
- Risk Assessment
- Risk Control
- Risk Communication

HKARMS

Define Safety Margin

- How safe is safe?
- Safety requirements specify that no unacceptable event shall occur during the lifetime of the system
- 1×10^6 hours MTBF is established as safety limit
- To Account for uncertainties and data variability
  - Any event with a brake rate less than 3 mphps is also subject to risk mitigation
  - Events with a brake rate less than 4 mphps should also be verified with testing or calculations

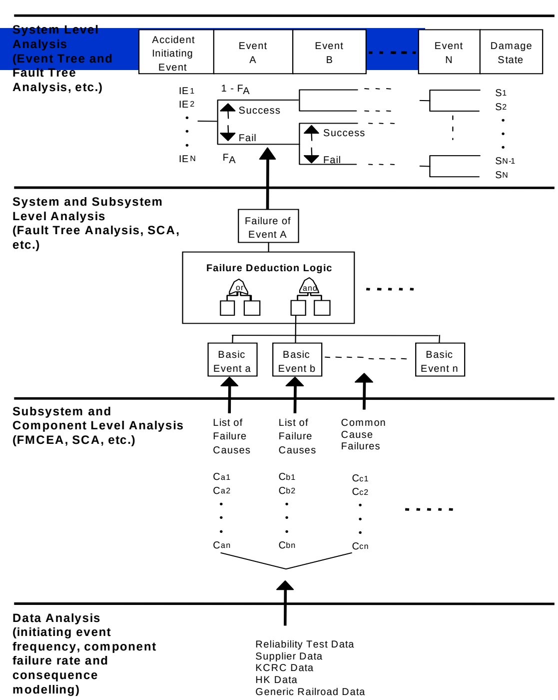
HKARMS



HKARMS

Risk Identification and Assessment

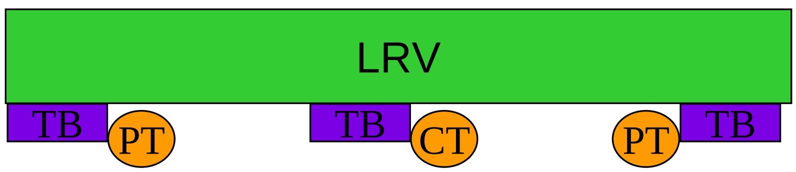
- Integrated Event Tree/Fault Tree analysis technique
- Postulate scenarios using event tree
- Determine system unavailability using fault tree



HKARMS

Postulate Scenarios

- Safeguards (safety barriers) are
  - M Out of 6 TBs Functional
  - N Out of 4 Power Truck Brakes Functional
  - R Out of 2 Center Truck FBs Functional
- All failure scenarios are considered
  - Evaluated 105 scenarios for all possible failure combinations, not just one or two “worst case” scenarios
  - Each with an expected likelihood and consequence
- Consequence is measured by the resulting brake rate
- Individual risk not assessed at this stage

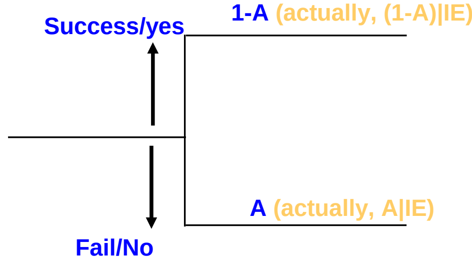


HKARMS

Postulate Scenarios Using Event Tree

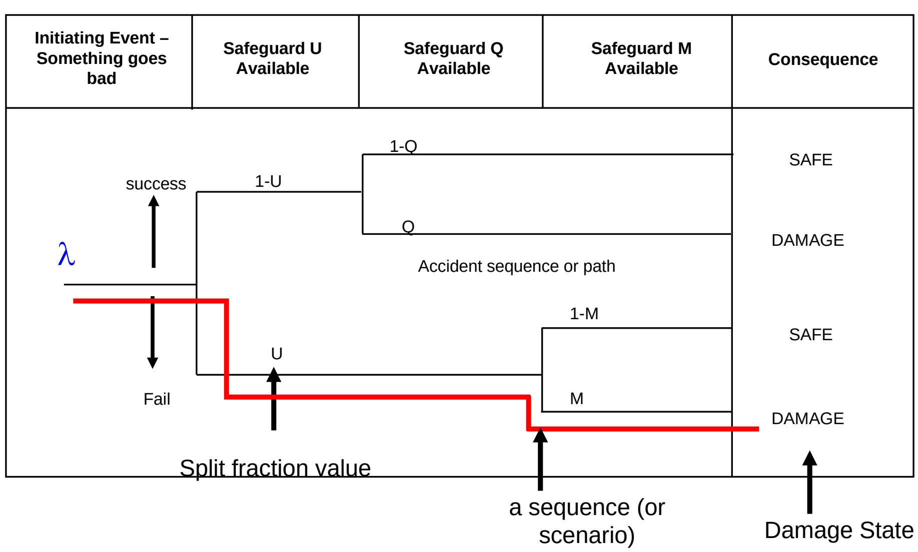
Event Tree Analysis

- Use inductive logic to postulate and quantify accident scenarios or accident sequences
- Start with initiating event and follow through scenario to identify possible scenarios



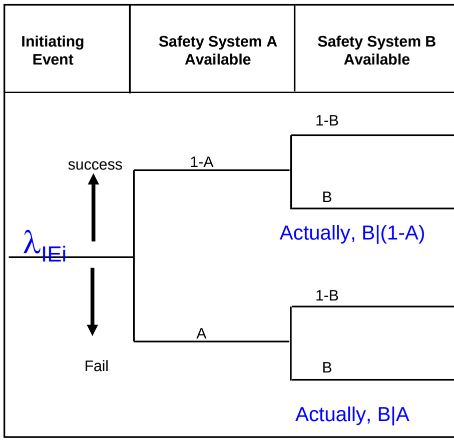
- “A” is a probability called the “split fraction”
- The sum of all split fractions coming out from a branch is 1

Probability of a Sequence



HKARMS

Event Tree Analysis



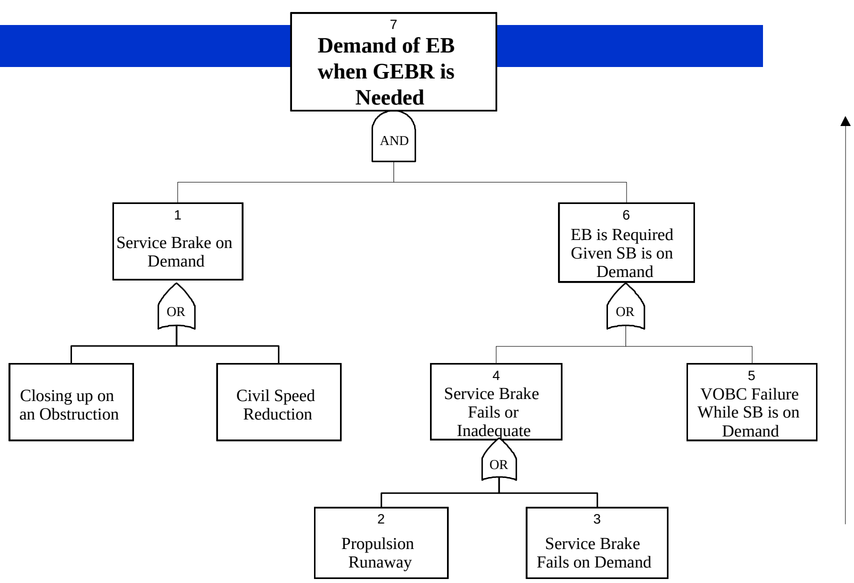
Consequence	Path Conditional Probability	Path Frequency	Path Risk
q_1	$p_1=(1-A)(1-B)$	$\lambda_1 = \lambda_{IE} p_1$	$R_1 = \lambda_1 q_1$
q_2	$p_2=(1-A)B$	$\lambda_2 = \lambda_{IE} p_2$	$R_2 = \lambda_2 q_2$
q_3	$p_3=A(1-B)$	$\lambda_3 = \lambda_{IE} p_3$	$R_3 = \lambda_3 q_3$
q_4	$p_4=AB$ $\Sigma=1$	$\lambda_4 = \lambda_{IE} p_4$	$R_4 = \lambda_4 q_4$

Total Risk for IE_i $\quad R_i = \lambda_{IEi} \Sigma R_{i|IEi}$

Total System Risk $\quad R = \Sigma_j (\lambda_{IEj} \Sigma_i R_i)$

HKARMS

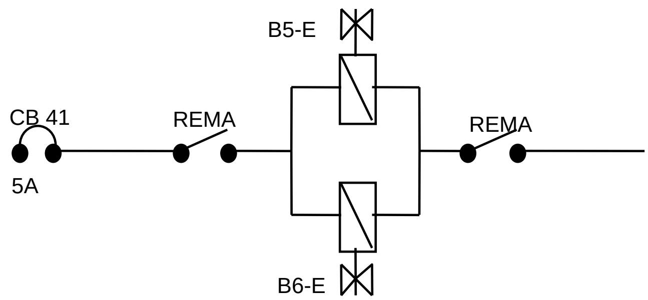
Initiating Event – Demand of EB



IE Frequency (λ) is Approximately 59 EB Demand/Year

Determine Friction Brake Unavailability

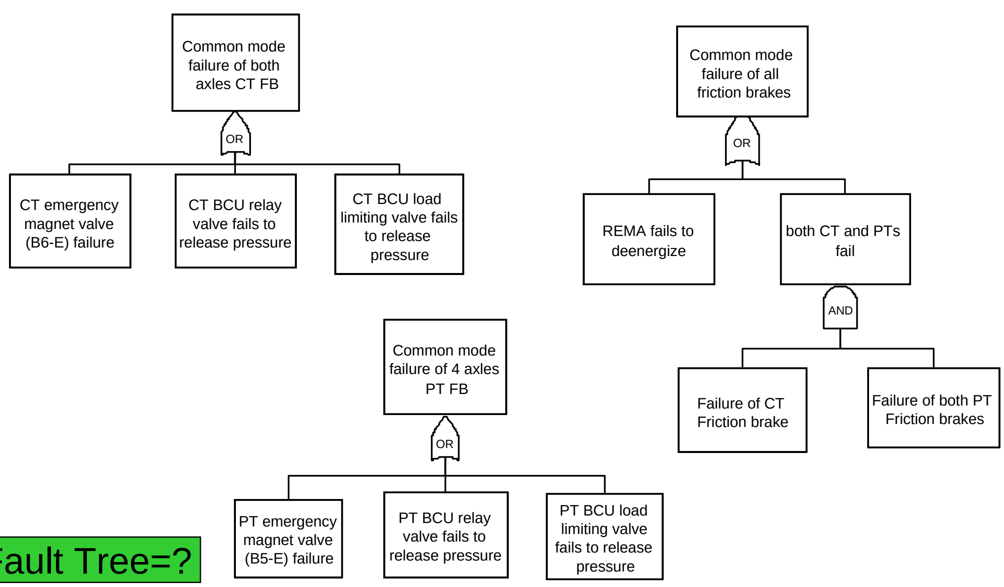
- FBs are controlled by two Emergency Brake Valves (EMVs), One for both sets of Power Truck Brakes and one for the Center Truck Brakes
- All FBs are controlled by REMA



E Valves are de-energise to activate emergency friction brake

REMA	Emergency Relay A
B5-E	Power Truck Emergency Magnet Valve
B6-E	Center Truck Emergency Magnet Valve

Determine Friction Brake Unavailability Using Fault Tree



Fault Tree=?

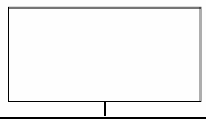
Fault Trees Analysis

- Can be qualitative or quantitative
- Start with Top Event (a failure event) and follow through scenarios that lead to the Top Event
- Use deductive logic to systematically identify event initiators
- Separate tree into functional level, system level, subsystem level, component level, fault level, etc.
- Bottom of the tree are basic events or developed events, usually with data available

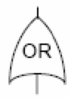
Fault Tree Symbols

- Two kinds of symbols are used in a fault tree:
  - Logic symbols
  - Event symbols
- Many symbols and styles, we stay with the simple ones here

Fault Tree Symbols

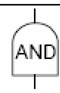


TOP Event – forseeable, undesirable event, toward which all fault tree logic paths flow,or **Intermediate event** – describing a system state produced by antecedent events.

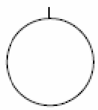


"Or" Gate – produces output if any input exists. Any input, individual, must be (1) necessary and (2) sufficient to cause the output event.

Most Fault Tree Analyses can be carried out using only these four symbols.



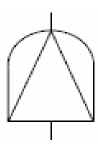
"And" Gate – produces output if all inputs co-exist. All inputs, individually must be (1) necessary and (2) sufficient to cause the output event



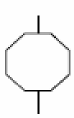
Basic Event – Initiating fault/failure, not developed further. (Called "Leaf," "Initiator," or "Basic.") The Basic Event marks the limit of resolution of the analysis.

Events and **Gates** are **not** component parts of the system being analyzed. They are symbols representing the logic of the analysis. They are bi-modal. They function flawlessly.

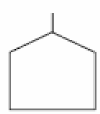
More Fault Tree Symbols…



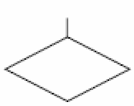
Priority AND Gate
$P_T = P_1 \times P_2$
Opens when input events occur in predetermined sequence.



Inhibit Gate
Opens when (single) input event occurs in presence of enabling condition.



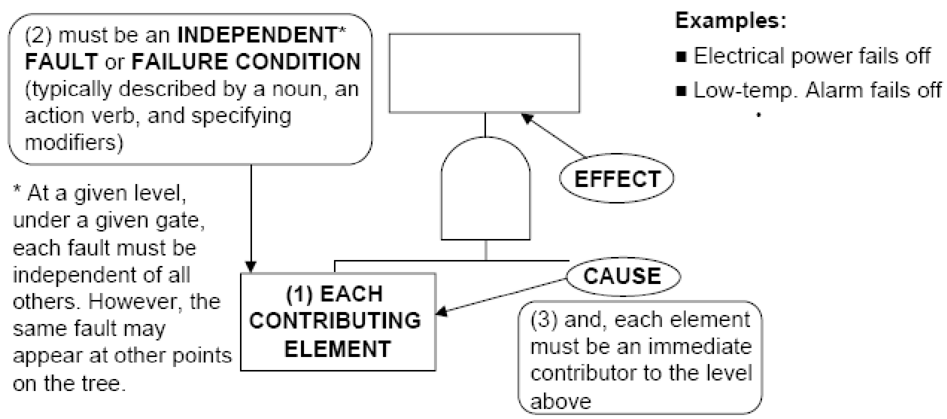
External Event
An event normally expected to occur.



Undeveloped Event
An event not further developed.

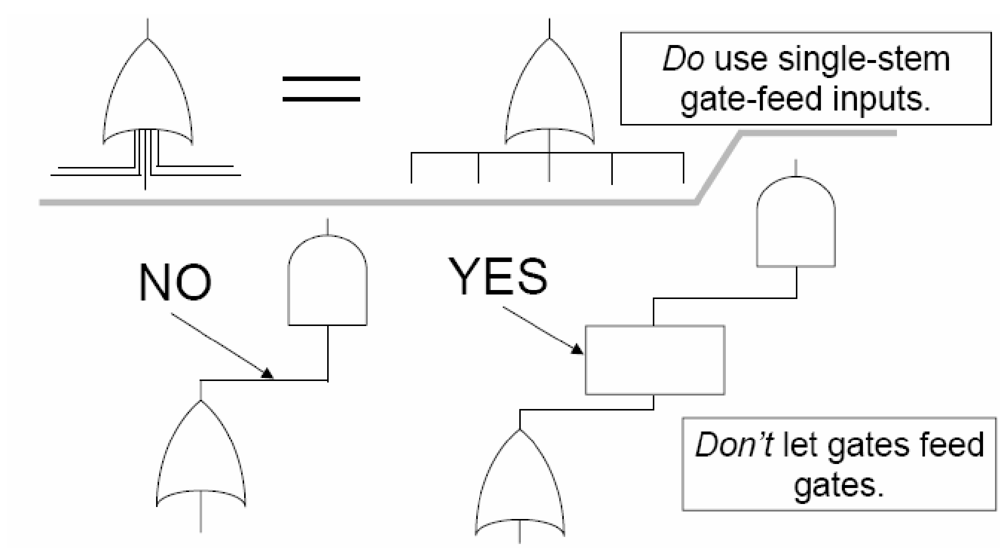
Conditioning Event
Applies conditions or restrictions to other symbols.

Relationship between the Fault Tree Symbols



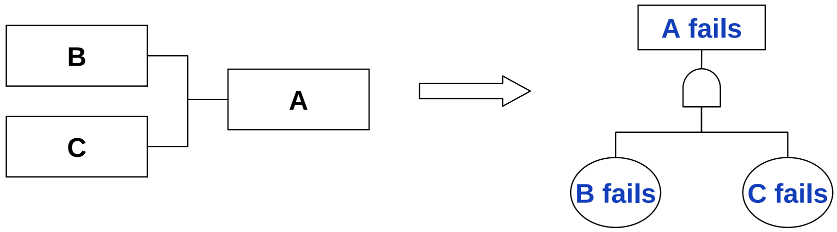
NOTE: As a **group** under an AND gate, and **individually** under an OR gate, contributing elements must be both **necessary** and **sufficient** to serve as **immediate** cause for the output event.

Fault Tree Symbols – Common Rules

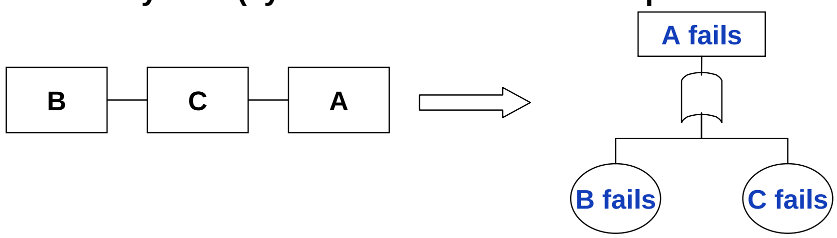


Fault Tree Structure

Event A occurs because of Event B and Event C occur
A parallel system (system works if either component works)

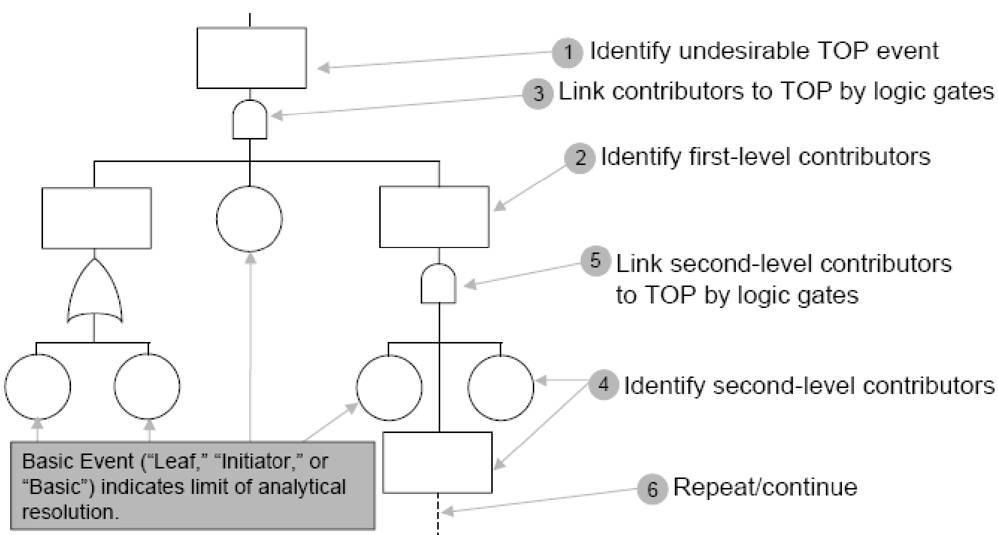


Event A occurs because of Event B or Event C occur
A series system (system works when all components work)



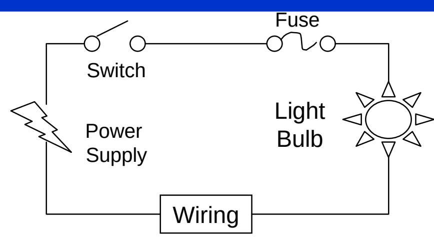
HKARMS

Fault Tree Construction



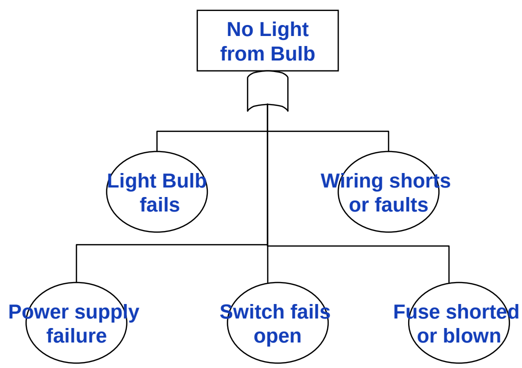
HKARMS

Fault Tree Structure, Example

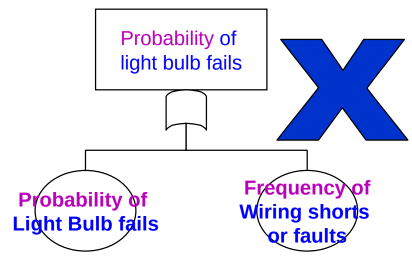


Develop fault event with top event: No light from bulb

Initial conditions: Switch closed
Not-considering events: failure external to system

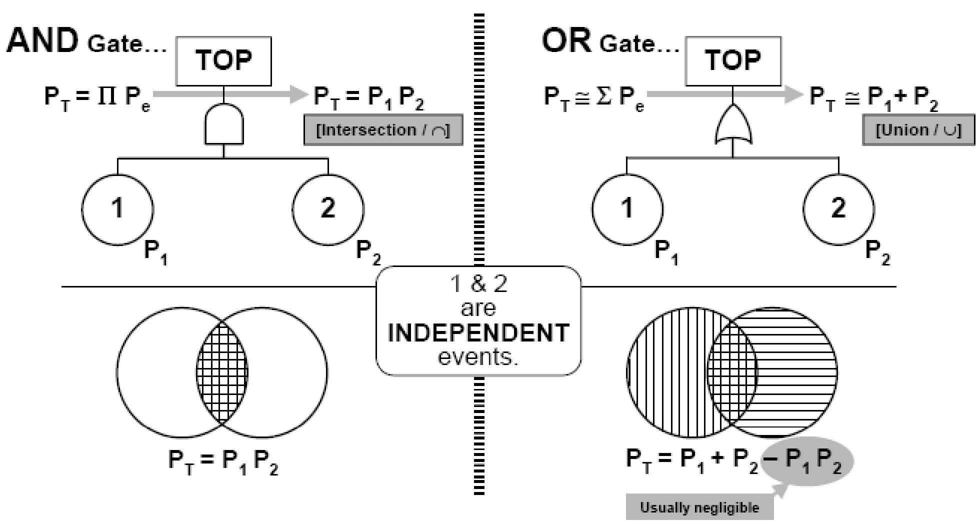


Do not put down:



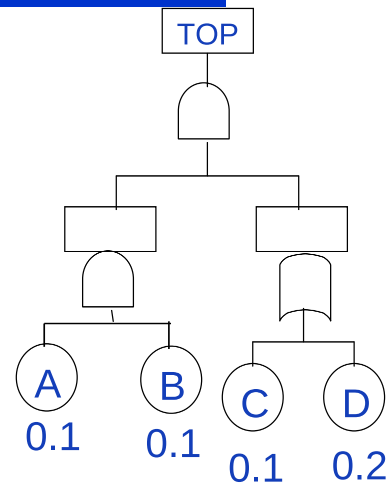
HKARMS

Fault Tree Calculations



Fault Tree Calculation

- Fault tree is based on probability theory in solving Boolean algebra
- Approximation:
  - P(Top) ≈ P(A) x P(B) x [P(C) + P(D)]
  - P(Top) ≈ 0.1x0.1x(0.1+0.2) = 0.003
- Exact:
  - P(Top) = P(A) x P(B) x [P(C) + P(D) – P(C)xP(D)]
  - P(Top) ≈ 0.1x0.1x(0.1+0.2 – 0.1x0.2) = 0.0028

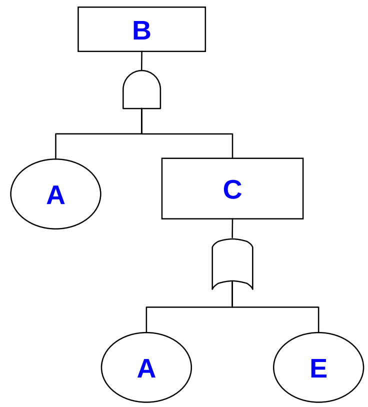


Events in a fault tree cannot be a frequency or anything that has a unit; otherwise, u*u-u

HKARMS

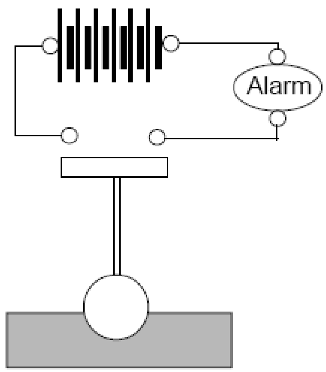
Fault Tree Calculation

- **A=0.1, E=0.2, What is B?**



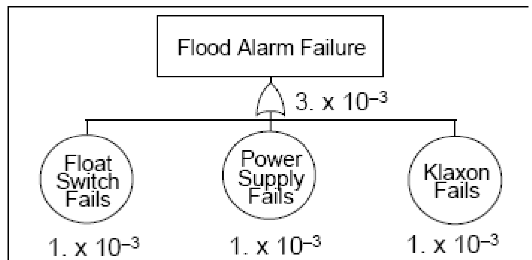
- **B= A* (A+E) = 0.1*(0.1+0.2) = 0.03**
- **B=A = 0.1 ????**

Example - A Flood Alarm System



A system design goal is $P_F < 5 \times 10^{-6}$, per flood.

A subgrade compartment is protected against flooding by a simple alarm system. Each of the three components shown has a failure probability of 10^{-3} per demand. What is the probability of failure to alarm upon flooding?



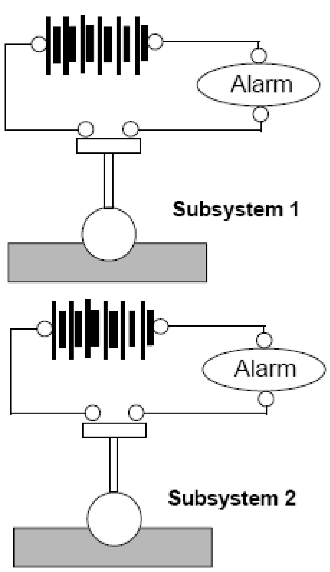
The system will fail three times in 1,000 demands, long-term average.

TOO MUCH RISK! So – go redundant.

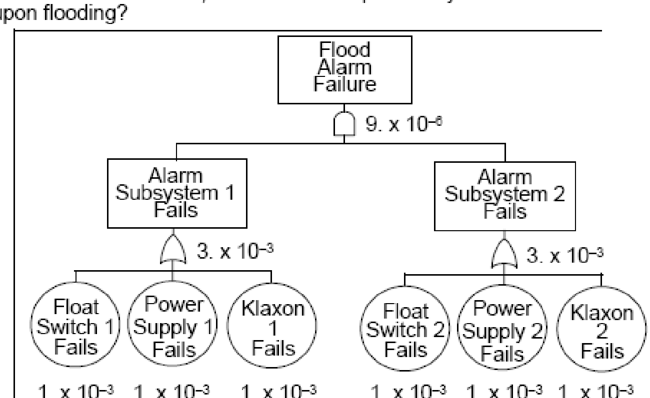
HKARMS

A Flood Alarm System

Two System Redundancy



Two subsystems identical to the first system are now used. Ignoring common-cause effects, what now is the probability of failure to alarm upon flooding?

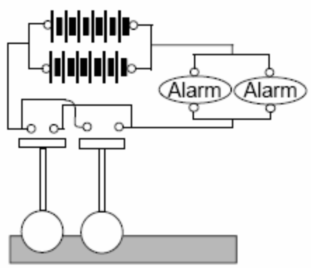


The system will fail 9 times in 10^6 demands…

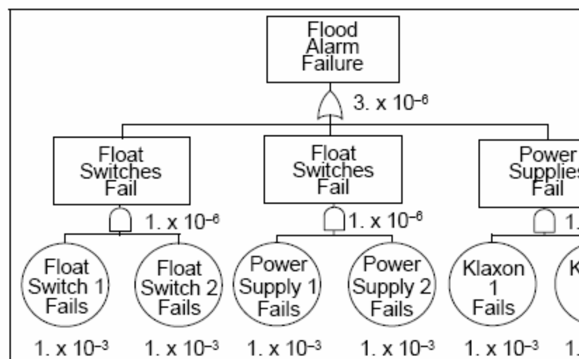
STILL TOO HIGH! Can it be further reduced, perhaps using the same components?

HKARMS

A Flood Alarm System
Component Level Redundancy



Components themselves are made redundant, rather than the whole system. What **NOW** is the probability of alarm failure upon flooding?

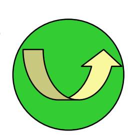


The system now fails 3 times in 10^6 demands – lower by a factor of three than for the previous case.

HKARMS

Typical Faults in Fault Tree Analysis

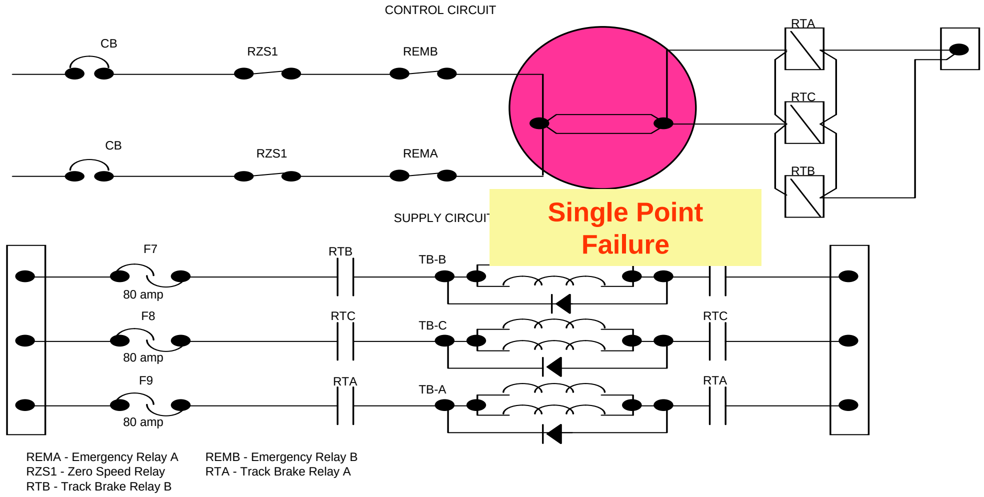
- Fault trees propagate probability or unavailability, NOT frequency
- Approximation led people to think they can add events together for “OR” gate regardless of contents
- Should not use fault tree simply to add events, A+B is not necessary A or B ;
  A or B = A + B – A*B



HKARMS

Determine Track Brake Unavailability

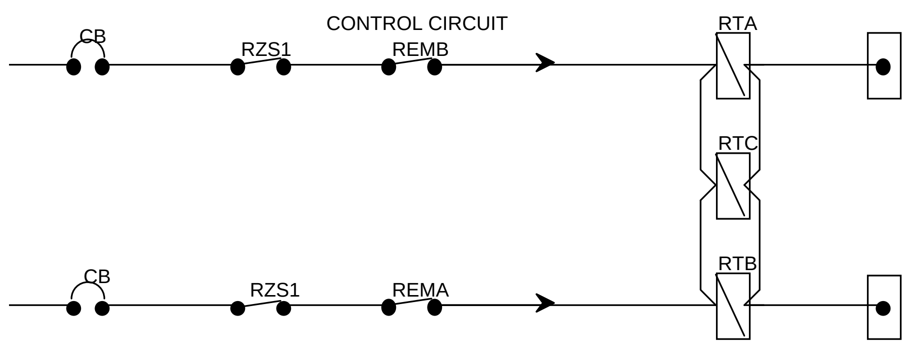
- TB Are Articulated Electromagnets Mounted on Springs Over the Rail Between the Wheels, Energized to Apply



HKARMS

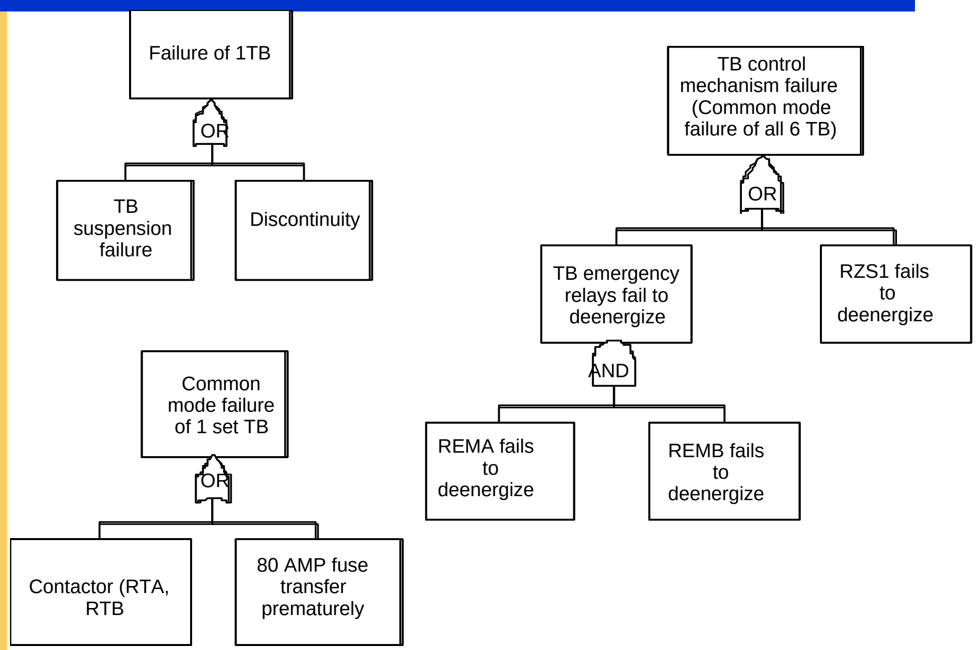
Determine Track Brake Unavailability

- Single Point Failure was identified during risk analysis and immediately eliminated by re-design



HKARMS

Determine Track Brake Unavailability Using Fault Tree



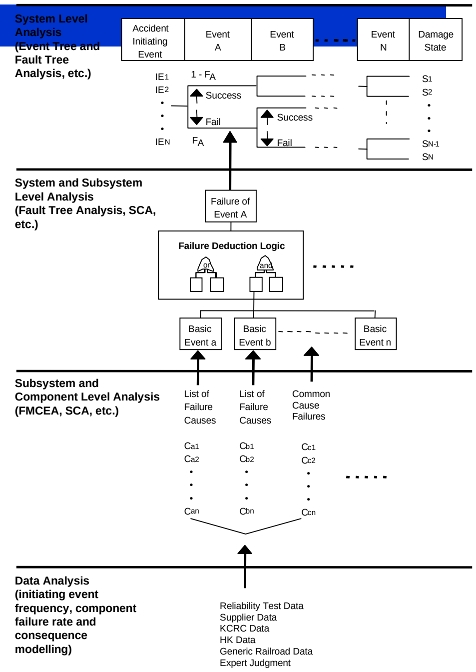
HKARMS

Brake Rates Used for Consequence Analysis

- The distribution of brake rate for the two Power Truck FBs and the Center Truck FBs are: 37.5%:37.5%:25%
- The TB brake rate for all 3 set of TBs (6 units) are assumed to be equally distributed

Brake Availability	TB	Power Truck FB	Center Truck FB
None available	0.00	0.00	0.00
1 Axle (FB) or 1 Unit (TB)	0.33	0.61	0.41
2 Axle (FB) or 2 Unit (TB)	0.66	1.23	0.82
3 Axle (FB) or 3 Unit (TB)	0.99	1.84	N/A
4 Axle (FB) or 4 Unit (TB)	1.31	2.45	N/A
5 Unit (TB)	1.64	N/A	N/A
6 Unit (TB)	1.97	N/A	N/A

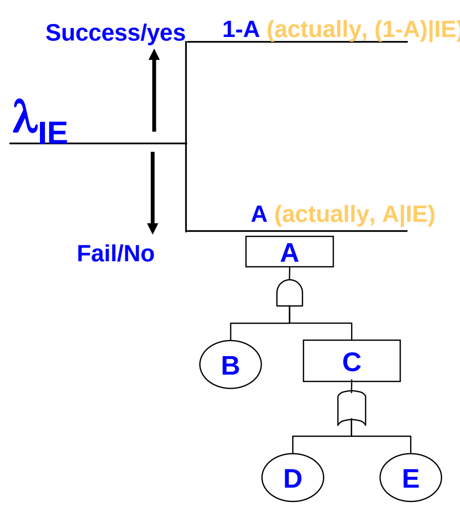
Conduct Event Tree/Fault Tree Analysis



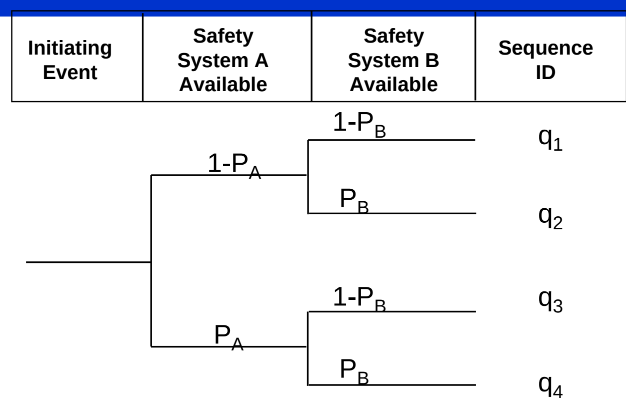
How??

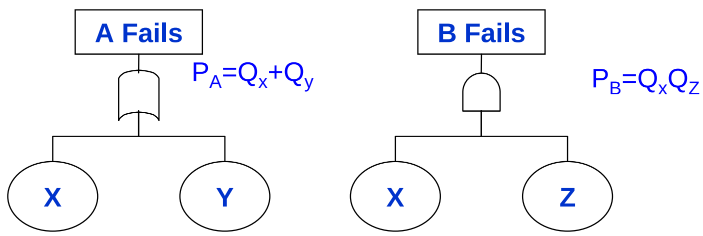
Integrated Event Tree/Fault Tree Analysis

- The split fraction of an Event Tree Heading "A" is The Top event unavailability of the fault tree used to model the failure of the Event "A"

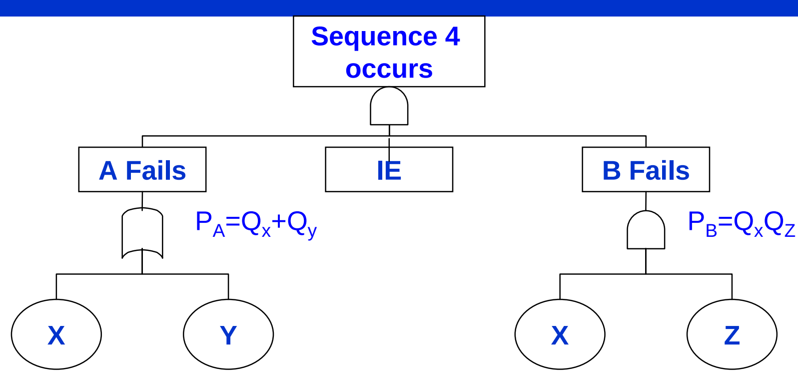


Integrated Event Tree/Fault Tree Analysis





Fault Tree Quantification

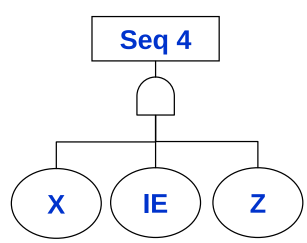


Top= IE*P_A*P_B

= IE (X+Y)(XZ)

= IE (XZ)

P (Sequence 4) = $\lambda_{IE}\, Q_x\, Q_z$



HKARMS

Risk Assessment Results

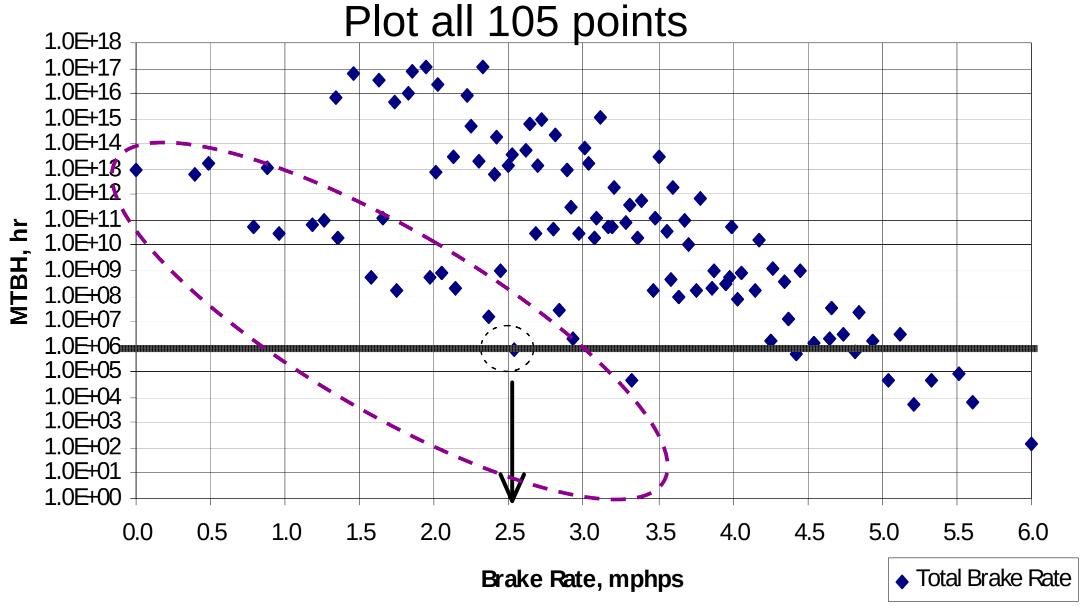
Scenario Number	m out of 6 TB Functional	TB Brake Rate	m out of 4 PT FB Functional	PTFB Brake Rate	r out of 2 CT FB Functional	CTFB Brake Rate	Total Brake Rate Achieved	Scenario Conditional Probability	IE (1/yr)	Total Scenario Frequency (1/yr)	MTTH (hr)
39	4 TB	1.57	2 PTFB	1.34	0 CTFB	0.00	2.91	4.49E-10	59.11	2.66E-08	3.30E+11
40	4 TB	1.57	1 PTFB	0.67	2 CTFB	0.96	3.20	8.36E-11	59.11	4.94E-09	1.77E+12
41	4 TB	1.57	1 PTFB	0.67	1 CTFB	0.48	2.72	1.51E-13	59.11	8.94E-12	9.80E+14
42	4 TB	1.57	1 PTFB	0.67	0 CTFB	0.00	2.24	2.70E-13	59.11	1.59E-11	5.50E+14
43	4 TB	1.57	0 PTFB	0.00	2 CTFB	0.96	2.53	9.19E-05	59.11	5.43E-03	1.61E+06
44	4 TB	1.57	0 PTFB	0.00	1 CTFB	0.48	2.05	1.66E-07	59.11	9.83E-06	8.91E+08
45	4 TB	1.57	0 PTFB	0.00	0 CTFB	0.00	1.57	2.96E-07	59.11	1.75E-05	5.00E+08
46	3 TB	1.18	4 PTFB	2.68	2 CTFB	0.96	4.82	2.30E-04	59.11	1.36E-02	6.45E+05
47	3 TB	1.18	4 PTFB	2.68	1 CTFB	0.48	4.34	4.16E-07	59.11	2.46E-05	3.56E+08
48	3 TB	1.18	4 PTFB	2.68	0 CTFB	0.00	3.86	7.41E-07	59.11	4.38E-05	2.00E+08
49	3 TB	1.18	3 PTFB	2.01	2 CTFB	0.96	4.15	8.33E-07	59.11	4.93E-05	1.78E+08
50	3 TB	1.18	3 PTFB	2.01	1 CTFB	0.48	3.67	1.51E-09	59.11	8.91E-08	9.83E+10
51	3 TB	1.18	3 PTFB	2.01	0 CTFB	0.00	3.19	2.69E-09	59.11	1.59E-07	5.51E+10
52	3 TB	1.18	2 PTFB	1.34	2 CTFB	0.96	3.48	1.13E-09	59.11	6.65E-08	1.32E+11
53	3 TB	1.18	2 PTFB	1.34	1 CTFB	0.48	3.00	2.04E-12	59.11	1.20E-10	7.28E+13

Quantified results available for all 105 failure scenarios

HKARMS

Risk Assessment Results Using Scattered Diagram

Plot all 105 points



Risk Assessment Results

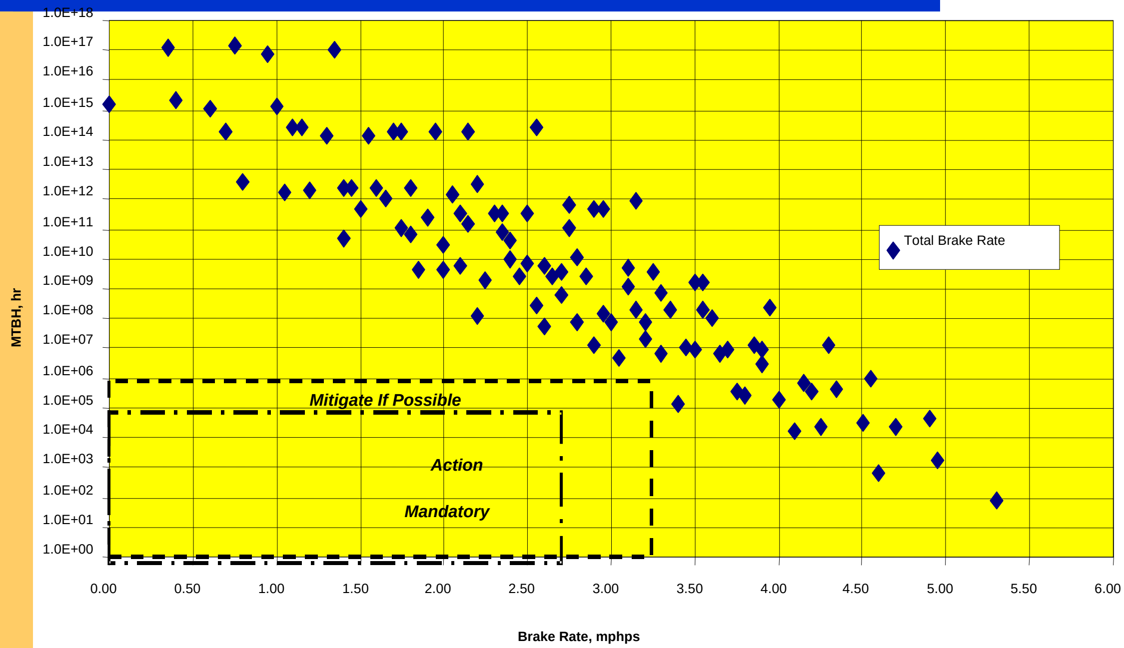
- GEBR = 2.5 mphps is marginally achievable
- Two groups of scenarios are identified; the lower constellation was generally associated with common mode failure of the Power Truck Brakes
- Four scenarios were identified to be the dominant risk contributors. All involve a common mode failure and single point failure that incapacitates all 4 axles of the Power Truck FBs
  - Scenario 43 Involves an Additional Failure of 2 TBs
  - Scenario 28 Involves an Additional Failure of 1 TB
  - Scenario 15 Involves the Additional Failure of 2 Center Truck FBs

Risk Management

- Options:
  - Accept the Current Risk Profile
  - Install Independent EM Valve in the FB System to Remove the FB Common Mode Failure
  - Increase Maintenance Frequency to Improve Reliability
  - Design the Train Control System With a Lower GEBR Specification
- Cost-Risk benefit Analyses would be performed to Identify Course of Action

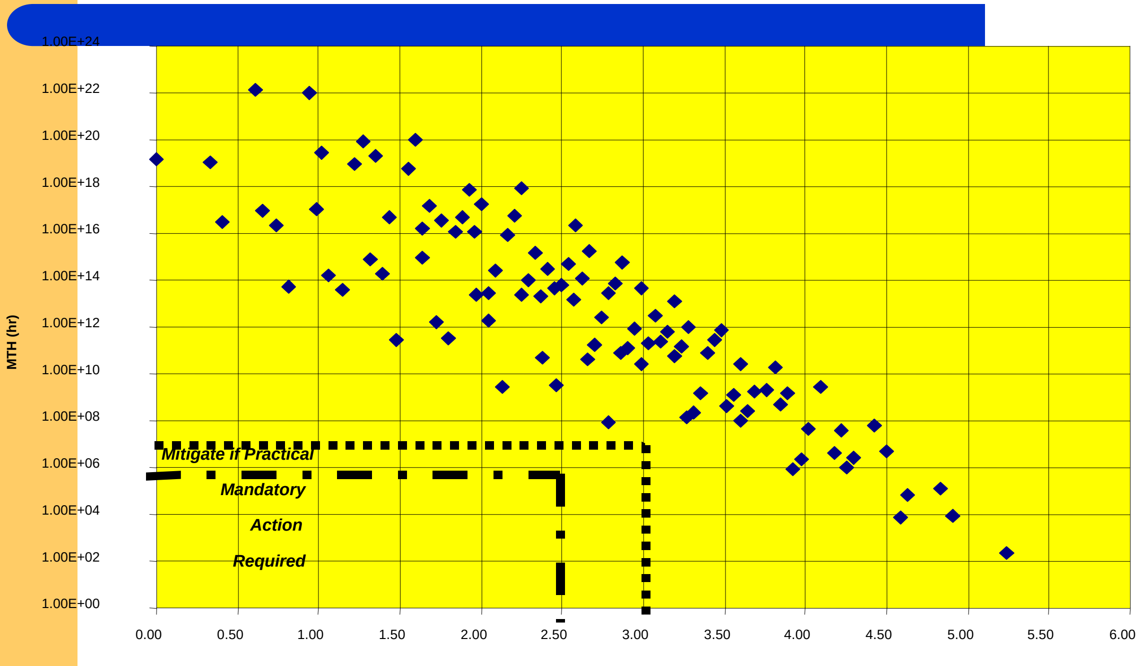
HKARMS

Risk Profile with Independent EM Valves



HKARMS

Risk Profile with EMV Inspection Period of 1 Hour – A Health Check Monitor



HKARMS

Conclusion

- A comprehensive risk analysis can provide information on the risk profile
- Scattered diagram have shown to be a good risk communication tool for this exercise
- Risk-informed decision is possible with a risk model

Q&A

For further enquires, please contact Vincent Ho

vsho@hkarms.org

END