CILTHK Joint Safety Seminar:

An Application of Quantitative Risk Assessment Techniques in Verifying System Safety Acceptance

Vincent Ho
22 August 2007

HKIE-SSC
HKIE-MMNC
HKARMS

1

Good Old Days…

- Railway – one of the most widely used public mass transportation modes
- Safety management is traditionally reactive, with focus on rules and procedures, passive safeguards and operator interventions
- Passengers exposed to involuntary risk
- Believed in setting unrealistic and unachievable goal – "zero accident"

2

Safety Analysis

- Traditional Transit Safety Analysis Tools
  - Checklist
  - Worst Case Analysis – Assume all brakes fail
  - Failure Chain – Arbitrary Pick a Scenario
  - Case Studies – Evaluate Past Accidents
- Issues:
  - What is "Worst Case?"
  - Are the analyses "credible"?
  - What is the Total Risk?
- Risk/Safety must be quantified before it can be improved

3

Quantitative Risk Assessment

- Historical Background
  - FMECA and RAM analyses in Aerospace Industry in the1960's and earlier
  - Probabilistic Risk assessment by nuclear power industries in mid 70's and 80's
  - Quantitative risk assessment in petrochemical industry in the 80's
- Issues:
  - The term "Risk" is not uniquely defined
  - Tools are not standardized (many reinventing the wheel)
  - Risk Analysis Versus Hazard Analysis

4

QR-What?

- Introduced to the railway industry in late 1980s
- The Railway (Safety Case) Act in UK
- Different terms have been used:
  - Probabilistic Risk Assessment (PRA)
  - Probabilistic Safety Assessment (PSA)
  - Quantitative Risk Analysis (QRA)
  - Quantified Risk Analysis (QRA)
  - Quantified Reliability Assessment (QRA?)
- Different consultants lead to different interpretations of risk and QRA

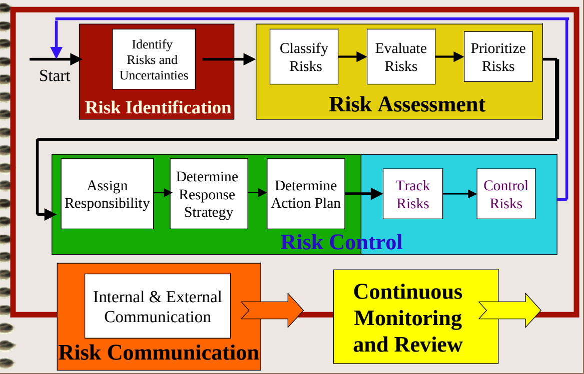
5

QRA

- What can go wrong?
- How likely is it?
- What are the consequences?
- What are the uncertainties?
- What is the total risk?

6

Key Steps in a QRA



7

Case Study:

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

8

Railway 101

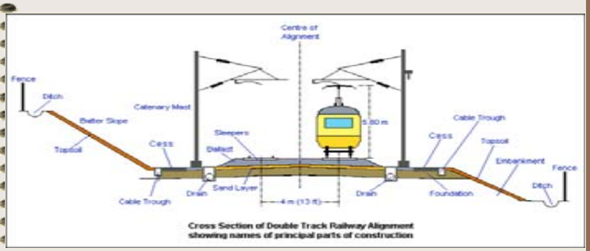
- Locomotives, EMU (not edible), diesel multiple units, ing stock
- Flags AWS, ATP,

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

9

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

10

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

11

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 (ATO, ATC)
  - Improved throughput (reduce headway)
  - Improve safety

12

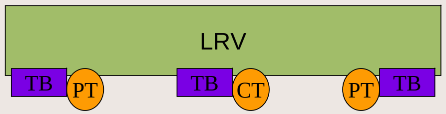
Guaranteed Emergency Brake Rate

- 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

13

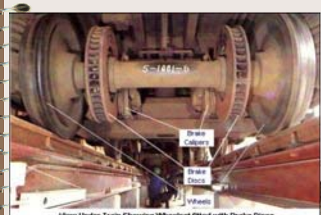
Braking System on these LRV

- 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)



14

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

15

GEBR Verification Procedures

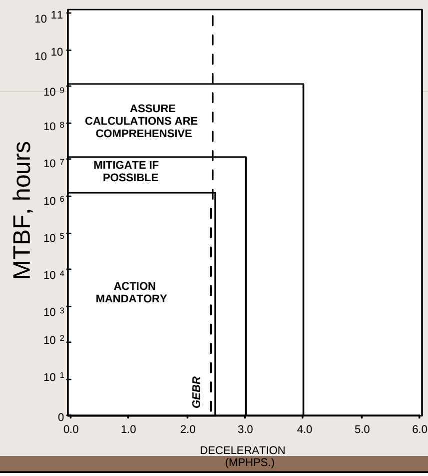
- Define Safety Margin
- Risk Identification
- Risk Assessment
- Risk Control
- Risk Communication

16

Define Safety Margin

- How safe is safe?
- Safety requirements specify that no unacceptable event shall occur during the lifetime of the system
- 1x10^6 hours MTBF is established as safety limit
- To Account for uncertainties and data variability
  - Any even[...] ps is also subject t[...]
  - Events w[...] should also be verifie[...]

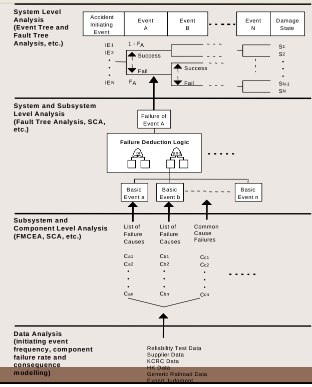
17



18

Risk Identification and Assessment

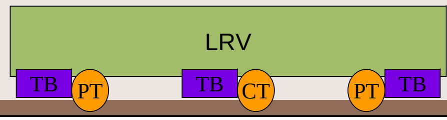
- Integrated Event Tree/Fault Tree analysis technique
- Postulate scenarios using event tree
- Determine system unavailability using fault tree



19

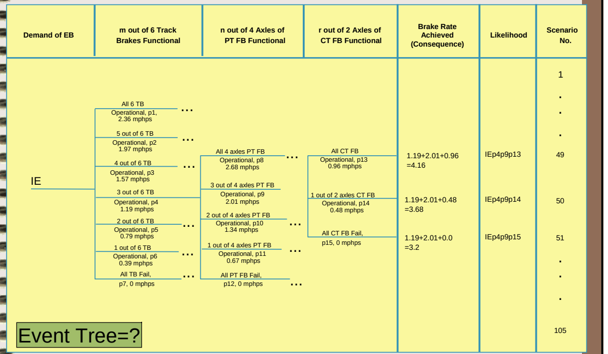
Postulate Scenarios

- 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



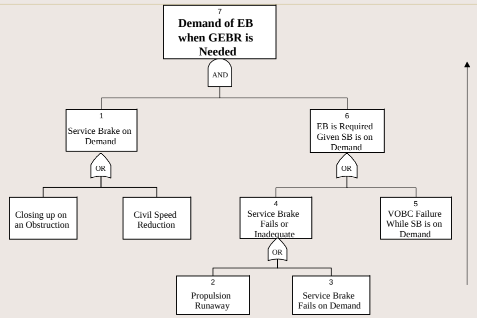
20

Postulate Scenarios Using Event Tree



21

Initiating Event – Demand of EB

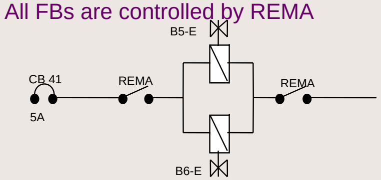


IE Frequency (λ) is Approximately 59 EB Demand/Year

22

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

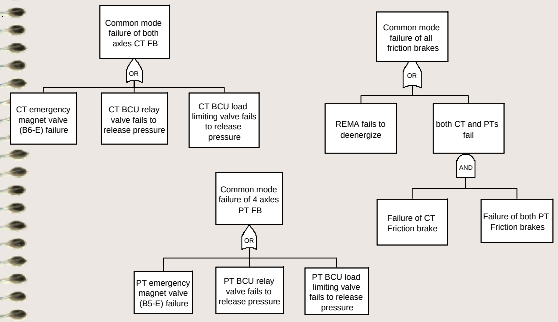


E Valves are de-energise to activate emergency friction brake

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

23

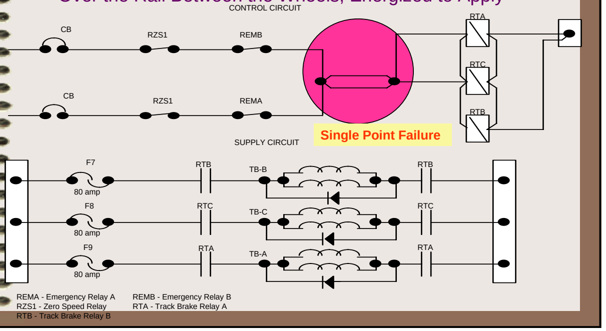
Determine Friction Brake Unavailability Using Fault Tree



24

Determine Track Brake Unavailability

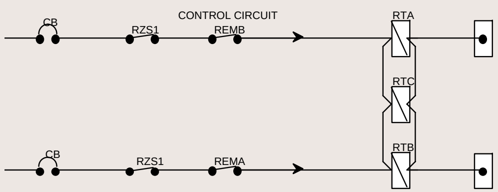
- TB Are Articulated Electromagnets Mounted on Springs Over the Rail Between the Wheels, Energized to Apply



25

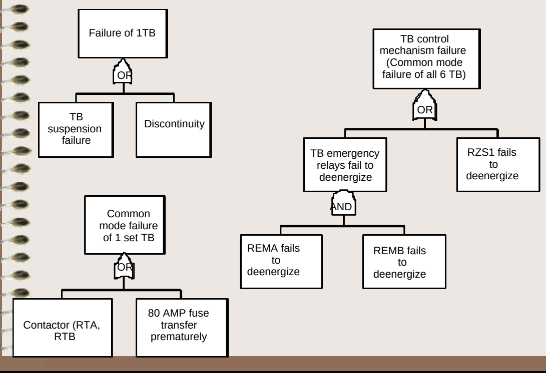
Determine Track Brake Unavailability

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



26

Determine Track Brake Unavailability Using Fault Tree



27

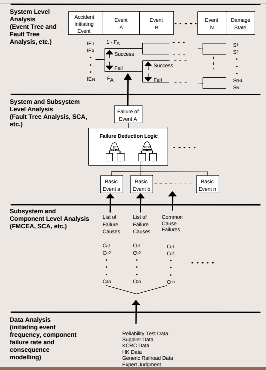
Brake Rates Used for Consequence Analysis

- 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

28

Conduct Event Tree/Fault Tree Analysis



How??

29

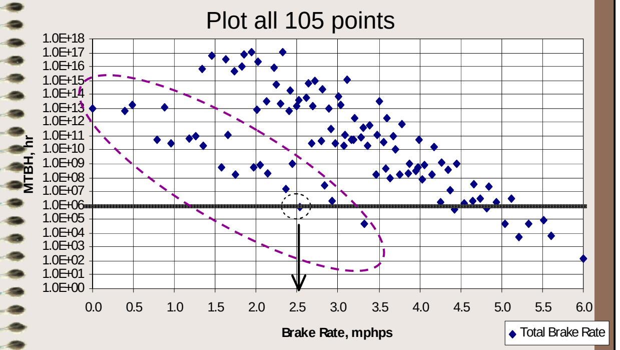
Risk Assessment Results

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

30

Risk Assessment Results Using Scattered Diagram



31

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

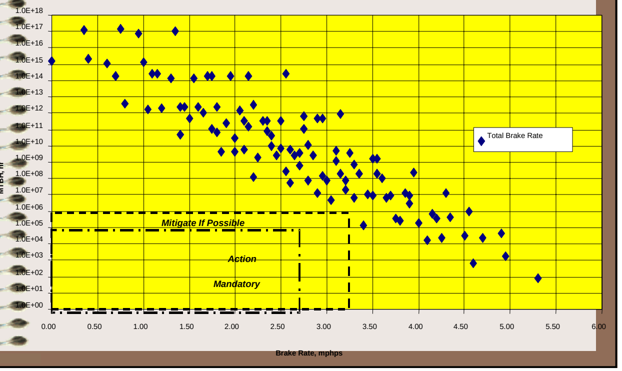
32

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

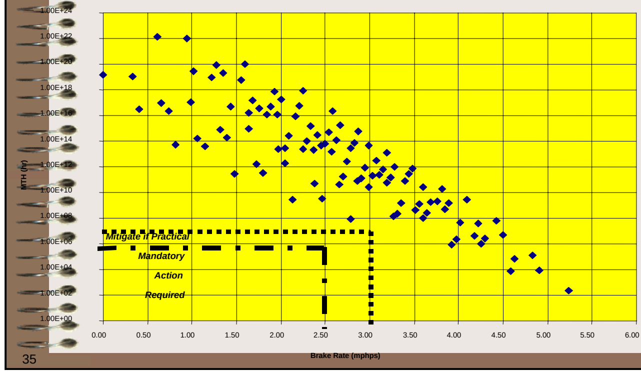
33

Risk Profile with Independent EM Valves



34

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



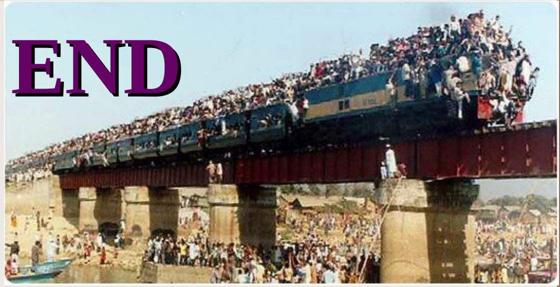
35

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

36

If there is no risk…



there is no opportunity.

37

Q&A

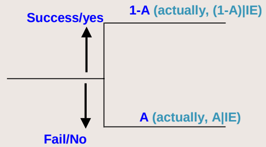
For further enquires, please contact Vincent Ho

vsho@hkarms.org

38

Event Tree Analysis

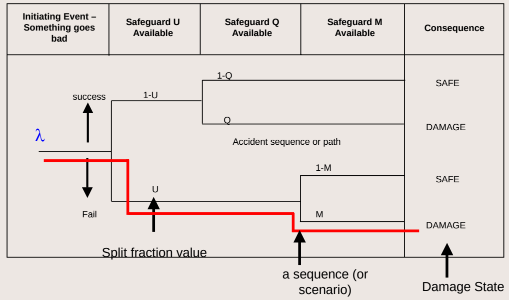
- Use inductive logic to postulate and quantify accident scenarios or accident sequences
- Start with initiating event and follow through scenario to identify possible scenarios



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

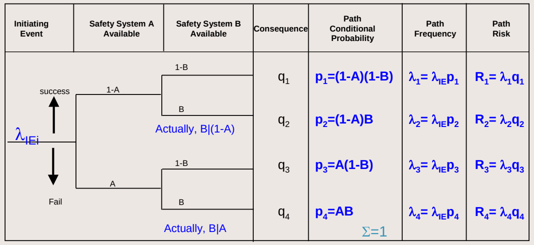
39

Probability of a Sequence



40

Event Tree Analysis



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

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

41

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

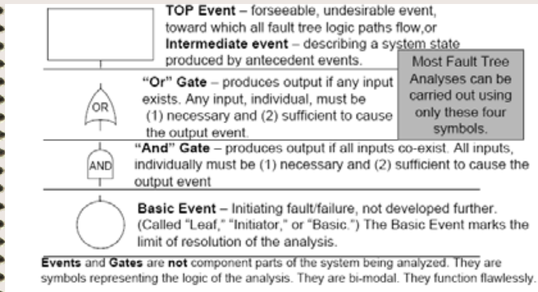
42

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

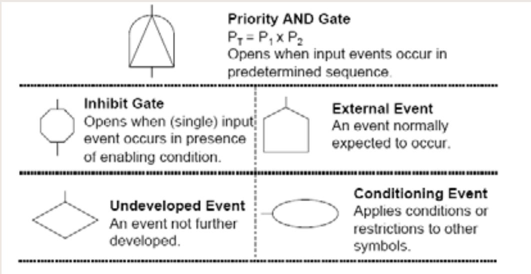
43

Fault Tree Symbols



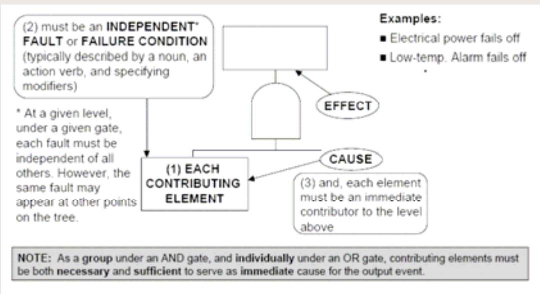
44

More Fault Tree Symbols…



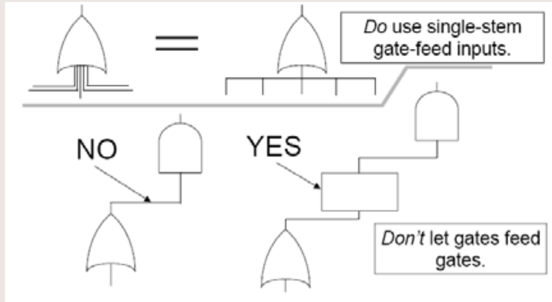
45

Relationship between the Fault Tree Symbols



46

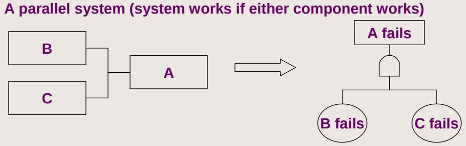
Fault Tree Symbols – Common Rules



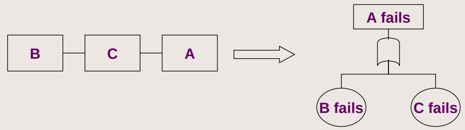
47

Fault Tree Structure

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

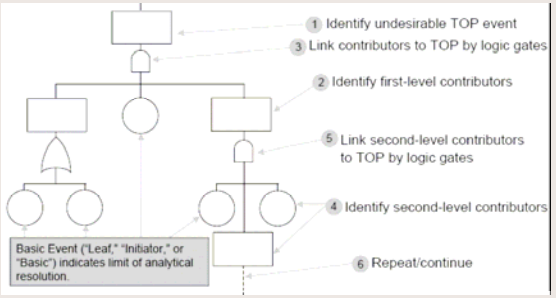


Event A occurs because of Event B or Event C occur
A series system (system works when all components work)



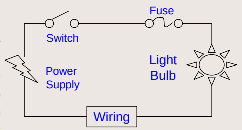
48

Fault Tree Construction



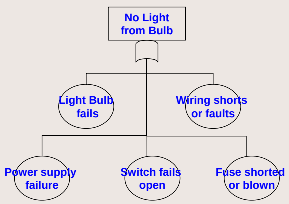
49

Fault Tree Structure, Example

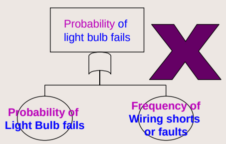


Develop fault event with top event: No light from bulb

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

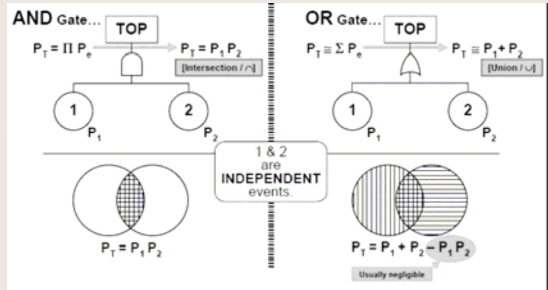


Do not put down:



50

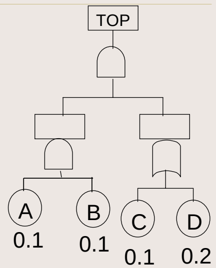
Fault Tree Calculations



51

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**

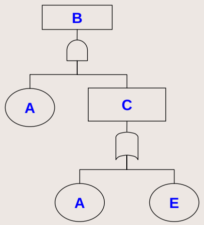


Events in a fault tree cannot be a frequency or anything that has a unit; otherwise, u*u-u

52

Fault Tree Calculation

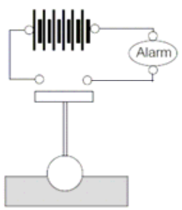
- A=0.1, E=0.2, What is B?



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

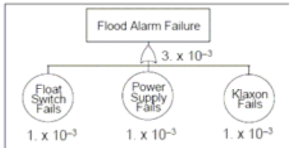
53

Example - A Flood Alarm System



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

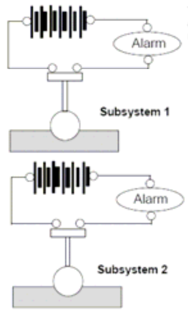
A subgrade compartment is protected against flooding by a simple alarm system. Each of the three components shown has a failure probability of 10^{-3} per demand. What is the probability of failure to alarm upon flooding?



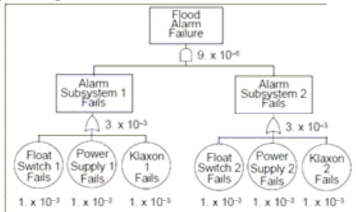
The system will fail three times in 1,000 demands, long-term average.
TOO MUCH RISK! So – go redundant.

54

A Flood Alarm System
Two System Redundancy



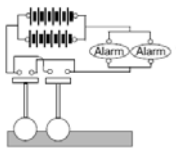
Two subsystems identical to the first system are now used. Ignoring common-cause effects, what now is the probability of failure to alarm upon flooding?



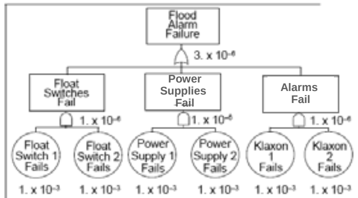
The system will fail 9 times in 10^6 demands.
STILL TOO HIGH! Can it be further reduced, perhaps using the same components?

55

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?

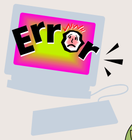


The system now fails 3 times in 10^6 demands – lower by a factor of three than for the previous case.

56

Typical Faults in Fault Tree Analysis

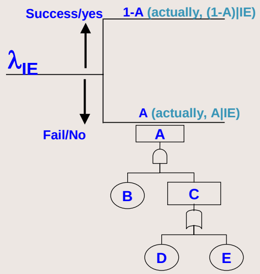
- Fault trees propagate probability or unavailability, NOT frequency
- Approximation led people to think they can add events together for "OR" gate regardless of contents
- Should not use fault tree simply to add events, A+B is not necessary A or B ;
  A or B = A + B – A*B



57

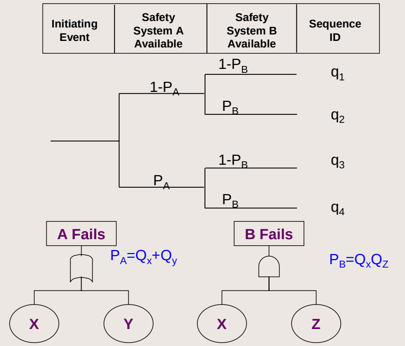
Integrated Event Tree/Fault Tree Analysis

- 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"



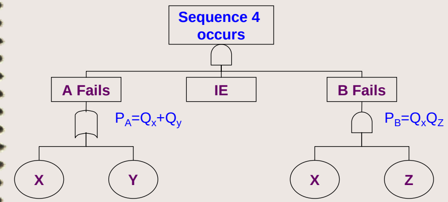
58

Integrated Event Tree/Fault Tree Analysis

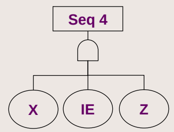


59

Fault Tree Quantification



$$\text{Top} = IE \cdot P_A \cdot P_B$$
$$= IE\,(X+Y)(XZ)$$
$$= IE\,(XZ)$$
$$P\,(\text{Sequence } 4) = \lambda_{IE}\, Q_x\, Q_z$$



60

A Risk-Based Approach to Verify the Guaranteed Emergency Brake Rate

Vincent Ho, Ph.D., P.E., C.S.P.;

Keywords: transit signaling, guaranteed emergency brake rate, event tree, fault tree, quantitative risk management

ABSTRACT

This paper describes a risk-based approach that uses proven probabilistic risk assessment techniques to verify the system safety acceptance of the emergency braking of a modern light rail vehicle supervised by an automatic train control system. The techniques and application of quantitative risk assessment (QRA) has been largely misunderstood and misapplied by non-safety trained engineers. This problem has been compounded due to the lack of dedicated safety engineers in the railway industry. This paper intends to illustrate the proper way of using the basic tools such as fault tree and event tree in a QRA for the railway industry.

Using an integrated event tree/fault tree risk model, all perceivable failure scenarios associated with the emergency braking system were objectively postulated, and their consequence and frequency of occurrence were individually quantified. The total risk associated with the emergency braking system was assessed. Using application examples, this paper illustrates that the risk-based approach can be an effective risk management tool. The approach can offer significant advantages over the "worst case analysis" approach commonly used in the transit industry to verify system safety.

INTRODUCTION

Railroad and light rail transit systems have traditionally used line-of-sight operating mode. The driver has the full responsibility to prevent accidents such as collision by regulating the vehicle speed and applying the brake when necessary. In order to provide a safer service, many transit systems rely on signaling to regulate train speed and movement authority. To meet the tremendous growth of ridership demand, transit signaling using automatic train control (ATC) becomes essential in densely populated areas.

Safe Braking Model

A fundamental aspect of transit signaling is the safe braking model. This model is used to determine the distance that must be maintained between vehicles and obstacles in order to avoid collisions. The distance separation translates into the time separation between trains, which is often known as the headway. A transit system with a shorter headway can transport more passengers within a given time if the system has enough trains to support the demand. Therefore the result of this model is important not only to the safety, but also the performance of a transit system.

The following are typical elements to be considered in a safe braking model:

- Initial recognition of signal change
- Reaction time
- Propulsion runaway
- Emergency brake application (EB)

- Vehicle Overhang

During an EB, the train is presumed to decelerate at a brake rate that is derived from a combination of measurement and conservative assumptions regarding braking system failures and wheel-to-rail adhesion. The brake rate that results in the largest component of the safe braking distance is commonly known as the Guaranteed Emergency Brake Rate (GEBR). Safety of a transit system can then be demonstrated by showing that the system can achieve the GEBR within an acceptable mean time between hazards.

Worst Case Analysis

Traditionally, the safe braking model is verified by the "worst case" analysis. This approach replaced the old railroad practice of simply adding a safety factor (typically, 35%) to the calculated stopping distance. A worst-case analysis would assume each subsystem or critical component experiences a single point failure that reduces the brake rate. These failures are presumed to occur concurrently within the same stopping sequence as the worst possible failure mode.

For example, any system that is energized to apply is assumed to fail to the non-applied state. Track Brakes (if equipped) are such a system. Track brakes are articulated electromagnets mounted on springs over the rail between the wheels. Upon energization, they are attracted to the rail and drag, contributing to train deceleration. A "worst case" model would conservatively assume these devices fail completely, thus a large portion of nominal brake rate is not credited for safe braking distance.

Another form of braking commonly discounted in the safe braking model is dynamic braking. This type of braking uses the electric motors as generators to produce resistive force. It is not considered in a worst-case model because when the emergency braking has been initiated, it is assumed that the propulsion has either already failed or would be cut off.

If track brakes and dynamic brakes are discounted, then friction braking, either tread or disk, is all that is left to provide the necessary brake rate. But friction braking is adhesion limited and therefore it must be less than or equal to the rate that the wheel/rail interface will support.

Safety analyses using the worst-case approach usually demonstrate that a system is safe because the probability associated with the worst-case scenario is very low. However, although this approach can somewhat alleviate the risk perception of a system by addressing the accident with the most severe consequence, it does not really offer any new information. Unless there are serious flaws in the design a scenario with the most severe consequence would inherently have a low probability of occurrence because it requires a series of independent failures to occur.

Unfortunately, the worst-case scenario may not always be one of the dominant risk contributors to the system due to its relatively low probability of occurrence. Thus, safety analyses using the worst-case approach may give a false sense of safety and a non-conservative, misleading conclusion. Furthermore, the revenue of the transit system will be affected because the system performance (headway) would be penalized by an overly conservative stopping distance based on the worst-case model.

In order to conduct a meaningful, cost-efficient risk management program, the risk contributors of a transit system must be identified and evaluated. The dominant risk contributor can then be either eliminated or mitigated by design improvement and/or administrative control to assure public safety.

Quantitative Risk Assessment

Quantitative risk assessment (QRA), also known as the probabilistic risk assessment (PRA), techniques offer a new look at safety analysis since the landmark study, the Reactor Safety Study (ref. 1), was published in 1975. Traditional safety analyses determine whether a system is "safe enough" or has adequate protection by assuring that the system design meets its qualitative and quantitative design specifications. QRAs address all potential accident sequences that can jeopardize safety and operation. This goes beyond design basis failures and includes low-probability-high-consequence events.

The QRA methodology is simple and straightforward but is complex in execution. A QRA uses logic tools to systematically and comprehensively postulate accident sequences associated with a complex engineering system, and determine the frequency of occurrence of the undesirable consequences for each individual sequence. Rigorous data analysis techniques, such as the Bayesian analysis technique, are often used to formally assess uncertainties.

To date, the QRA approach has been used frequently in the nuclear power, aerospace, chemical/petroleum, and defense industries. The QRA approach is preferred over other safety analysis methods because it provides a better understanding of the overall risks associated with complex engineering systems. It can be used for making rational trade-off decisions when safety improvements are proposed. Since safety cannot be directly quantified, the risk associated with a system must be assessed instead to register the performance of a system. This paper presents a methodology based on QRA tools to verify the safe braking model. Application examples are used to demonstrate the use of an integrated event tree/fault tree model to assess the risk associated with the GEBR. Risk-Based System Safety Methodology

Definition of Risk

Risk has been defined in various ways in different industries, and is often misunderstood. For a complex engineering system analysis, risk analysis is used to answer the following questions:

- 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, and uncertainties.

Scenario

A scenario, or accident sequence, is used to address the first question: "What can go wrong?" Each accident sequence is unique in their likelihood and consequence. A scenario consists of three elements (in consecutive order):

- An initiating event which triggers the accident,

- The progression of the accident (success or failure of different events that affect the outcome of the accident) and
- The end state (consequence).

Following an initiating event in a typical risk analysis, there can be hundreds to millions of accident sequences, depending on the number of events that can affect the outcome of the sequence.

The event tree is an inductive graphical tool commonly used to systematically postulate and organize accident scenarios. Each branch of the event tree represents an accident sequence. It must be noted that because there can be more than two outcomes of an event, each event tree fork may split into more than two branches.

Likelihood

Mathematically, the associated risk can be expressed as:

$$R = \Sigma_i \, IE \, F_{i \mid IE} \quad (1)$$

Where IE is the frequency of the initiating event and F is the conditional probability for scenario i given the occurrence of the initiating event.

The probability of the branching is known as the split fraction. Fault tree models or engineering calculations are used to determine the values of the split fractions. The conditional probability of the system failure of an accident sequence is then simply the product of all split fractions that dictate the sequence.

Consequence

An end state can be either a safe state or a damage state, which can be further subdivided into different damage classes to distinguish the different levels of severity. The severity of the damage states depends on the outcome of the events in the event tree.

Uncertainties

There are three types of uncertainties associated with a risk model:

- Stochastic uncertainties
- Modeling uncertainties
- Parameter uncertainties

This paper will concentrate on the deterministic aspect of a risk model, and uncertainties will not be discussed in this paper. Figure 1 illustrates the relationship of the components of an integrated event tree/fault tree model.

The Analysis Process

The analysis consists of the following steps:

- Risk identification
- Risk evaluation
- Risk management

In the first step, risk identification, the safety acceptance criteria must be defined. The initiating event and the events that can affect the outcome of an initiating event are identified and arranged in a logical manner in the event tree. In the second step, risk evaluation, the components and subsystems that can affect the outcomes of an event are modeled by fault tree to obtain the failure probabilities or split fraction values (F_A in figure 1). The consequence of each sequence is also determined.

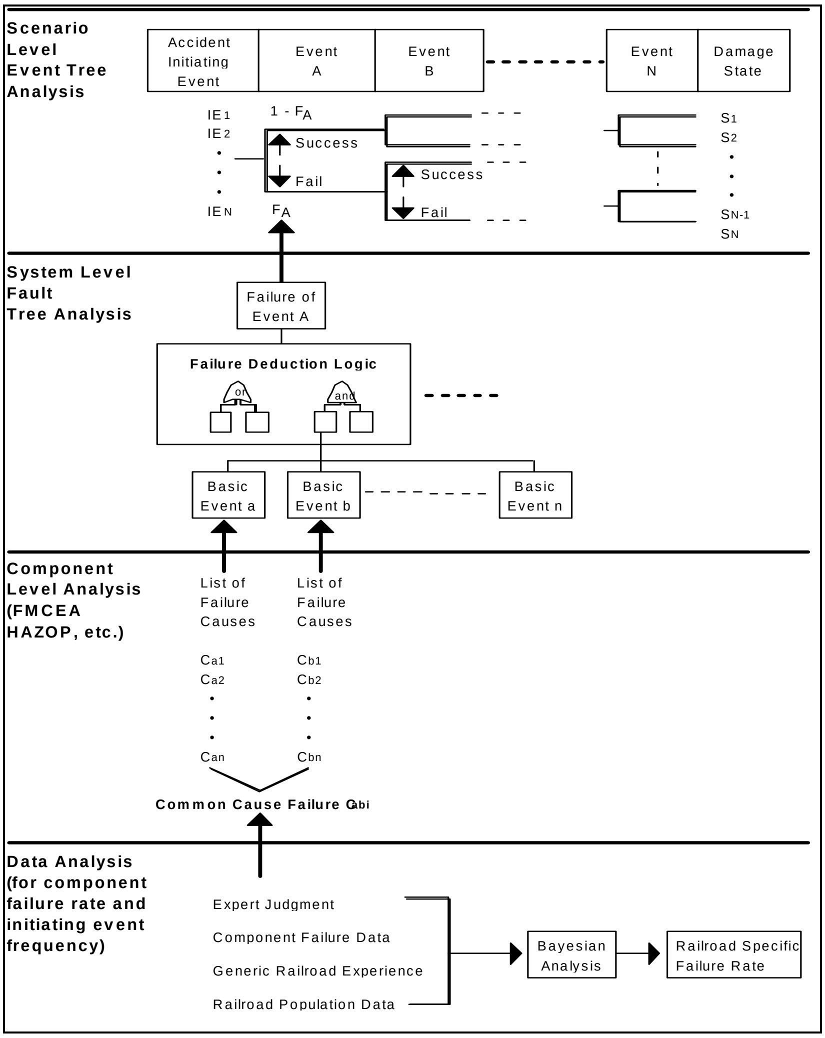


Figure 1 - Integrated Event Tree/Fault Tree Risk Model

The last step, risk management, prioritizes the risk impact of the accident sequence. The dominant risk contributors can then be identified. Those scenarios that are considered unacceptable based on the safety criteria can be analyzed further to determine the best course of action to reduce the risk impact. Simplified examples are provided below to illustrate the application of the model.

EXAMPLE 1 – GEBR DETERMINATION

This example determines the GEBR of light rail vehicles (LRV) regulated by an automatic train control (ATC) system. A comprehensive GEBR risk model is first developed. This model can be either used to verify the safety acceptance of a predetermined GEBR, or to determine a GEBR that satisfies a set of predetermined safety acceptance criteria. This example illustrates the latter application.

Risk Identification

The first step of a sound risk analysis is to address the question "How safe is safe?"

System safety acceptance criteria must be established to gauge the system performance before risk management actions can be taken. For illustration purposes, this example assumes that it is acceptable to have the Mean Time between Hazard (MTBH) of a single hazard be at least 10^6 hours for a fleet of 100 vehicles.

Initiating Event

GEBR is needed in an ATC system to maintain a safe stopping distance. During normal operation, dynamic brake and full service brake (FSB) are used to stop the LRV. EB is required if all these braking systems fail on demand, or when the ATC system commands an EB (e.g., ATC system failure). Thus, not all EBs require the same stopping distance be met. The initiating event would be Demand of EB that requires GEBR (when the LRV is closing upon an obstruction or civil speed reduction is required.)

Emergency Braking System

We assume the emergency braking system of the LRV consists of 2 power trucks (PT) and 1 unpowered center truck (CT) of friction brakes (FB), and 3 trucks of track brakes (TB). Each truck consists of 2 axles of brakes. For simplification, we assume the LRVs operate in a subway environment and adhesion of 16% can always be achieved and will be ignored in the consequence analysis.

Brake performance tests on the EB system measured the following brake rates:

Brake Component	Brake Rate, mphps
1 Axle of TB	0.39
1 Axle of PT FB	0.67
1 Axle of CT FB	0.48

Event tree Development

A multiple-branch event tree is then created to postulate all perceivable failure scenarios that can degrade the EB braking performance. Based on the combination of success and failure of the FB and TB, 105 accident sequences are identified in figure 2.

Risk Evaluation

In this example, we assume the frequency of the initiating event is 60 EB/yr for the fleet. Figure 2 shows the consequence (degraded brake rate) and the likelihood formula of each accident sequence.

Fault Tree Development

Fault trees are then developed to model the failure of the FB and TB. The top event probability of the fault trees will be used to calculate the split fraction values of the event tree. Figure 3 shows the fault trees developed to model the failure of 1 axle TB, 1 truck TB and the common mode failures of all TB. Similar fault trees can also be developed for the PT FB and CT FB (figure 4). It must be noted that the 3 trucks TB are controlled by 3 independent control and power supply circuits, while the 3 trucks FB are controlled by only 2 relays and 2 emergency brake magnet valves. A common mode failure that can fail both PT FB exists.

Data Analysis

The basic event of the fault tree depends on the failure rate and the inspection intervals of the components. Since the event tree in figure 2 has multiple branches, care must be taken to calculate the split fractions as compared to the typical binary-branched event. The split fractions for all branches in the event tree can be calculated. Table 1 shows a sample of the calculation results for selected sequences.

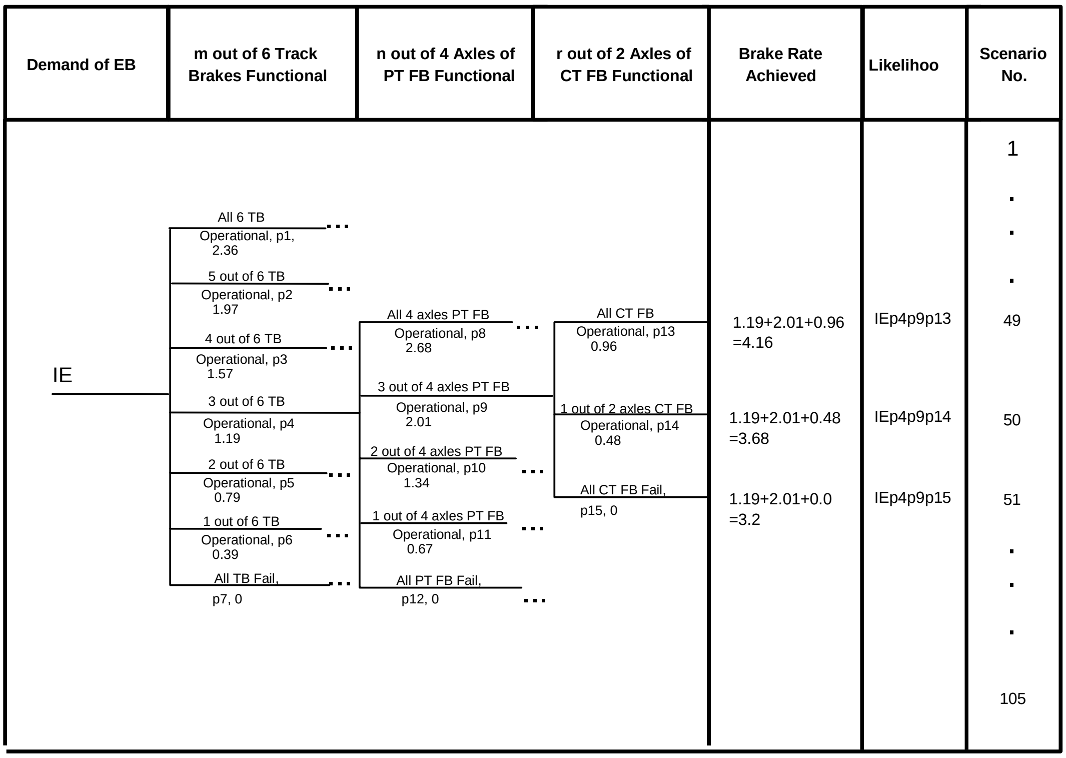


Figure 2 - Event Tree for the GEBR Model (3 complete sequences are shown).

Risk Management

The results of the 105 scenarios can be plotted in a scatter diagram (figure 5). The diagram shows two distinct groups of scenarios due to the dominating common mode FB failure (the lower left group). The safety acceptance limit of 10^6 hr of MTBH is also drawn on the scatter diagram.

The GEBR that satisfies the safety acceptance limit is determined by the scenario closest to the origin under the 10^6 limit line. This scenario is circled in figure 5. The corresponding brake rate is 2.55 mphps. Thus, a GEBR of approximately 2.5 mphps can satisfy the safety acceptance criteria.

The analysis shows that the scenario that has the greatest risk impact involves the failure of 2 PT FBs and 2 TB units. It is noted that the dominant risk contributors do not include the typical worst-case analysis scenario that requires failure of all FBs and TBs (with a MTBH of 10^{13} hr). The total frequency for all scenarios not meeting a 2.5 mphps GEBR is $5.5\text{x}10^{-4}$/yr.

Once the comprehensive GEBR risk model is developed, the risk associated with different configurations of the EB system can be assessed. The following example addresses the addition of a third EM valve to the FB system.

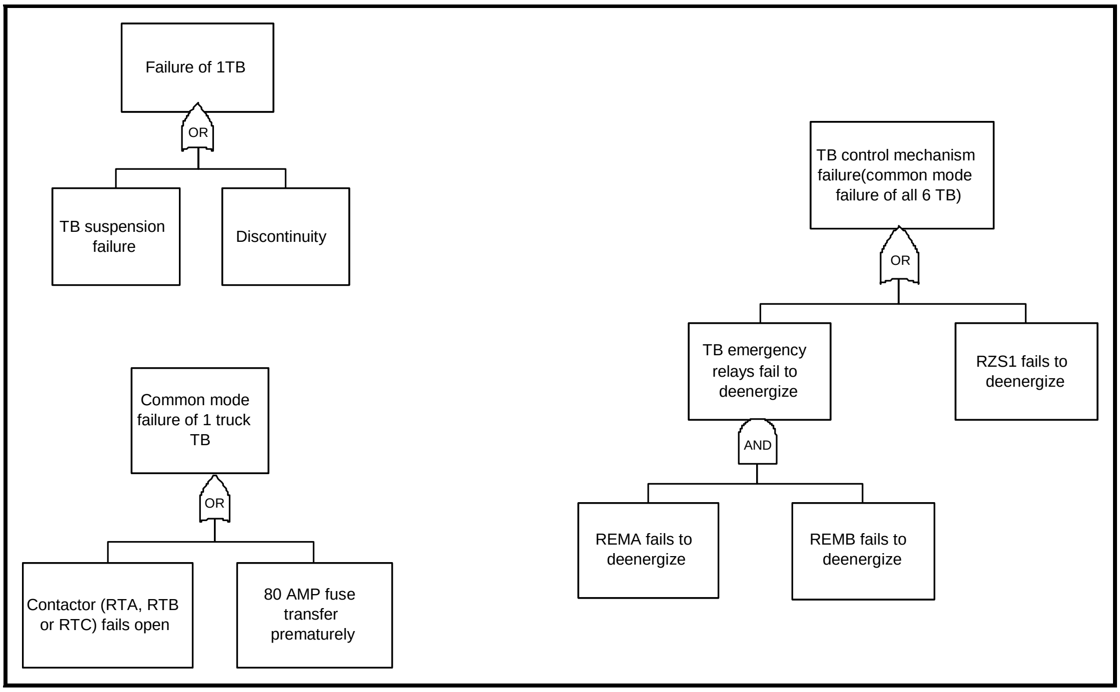


Figure 3 - Simplified Fault Tree for Track Brake Failure

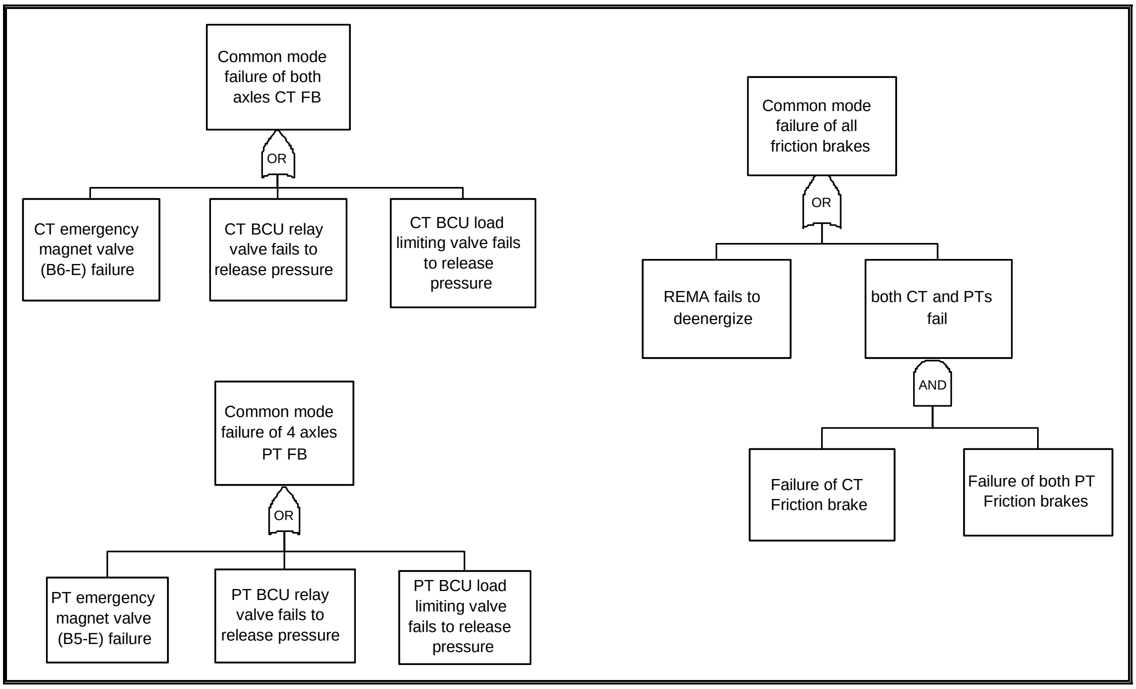


Figure 4 - Simplified Fault Tree for Friction Brake Failure

EXAMPLE 2 - COMPARE DIFFERENT BRAKE DESIGNS

The comprehensive GEBR risk model can be used to investigate the risk benefit of using a 3-valve friction brake system instead of 2 emergency brake magnet valves (EM valve).

Risk Identification

The safety acceptance criteria, the initiating event, and the event tree structure remain the same as the previous example.

Table 1 - Sample of Event Tree Calculation

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	Scenario Conditional Probability	IE (1/yr)	MTTH (hr)
47	3 TB	1.2	4 PTFB	2.7	1 CTFB	0.5	4.3	4.16E-07	60	4.01E+04
48	3 TB	1.2	4 PTFB	2.7	0 CTFB	0.0	3.9	7.41E-07	60	2.25E+04
49	3 TB	1.2	3 PTFB	2.0	2 CTFB	1.0	4.2	8.33E-07	60	2.00E+04
50	3 TB	1.2	3 PTFB	2.0	1 CTFB	0.5	3.7	1.51E-09	60	1.11E+07
51	3 TB	1.2	3 PTFB	2.0	0 CTFB	0.0	3.2	2.69E-09	60	6.20E+06
52	3 TB	1.2	2 PTFB	1.3	2 CTFB	1.0	3.5	1.13E-09	60	1.48E+07
53	3 TB	1.2	2 PTFB	1.3	1 CTFB	0.5	3.0	2.04E-12	60	8.19E+09

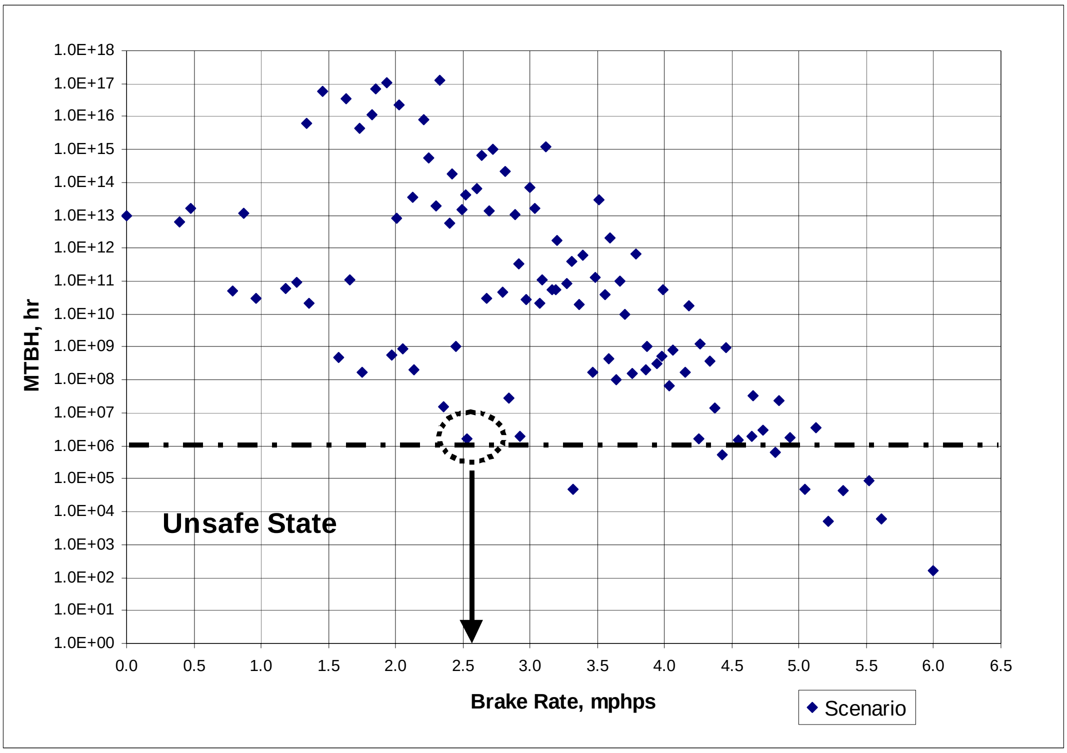


Figure 5 - The Risk Profile of the Accident Scenarios in Example 1

Risk Evaluation

The fault tree for the FB is modified to model the presence of an additional EM valve. The split fraction values for the FB branches are modified accordingly. Figure 6 shows the scatter diagram plot for scenarios in this example. The data no longer scatter into two groups as in figure 5.

Risk Management

Based on the result of the model for the alternative design, the risk of not achieving an effective brake rate is significantly reduced (see figure 6). This is mainly because the common mode failure that can fail all PT FBs has been eliminated.

The total frequency for all scenarios not meeting a 2.5 mphps GEBR with the 3-valve FB system is 3.3×10^{-6}/yr. Although the risk associated with the original 2-valve FB system meets the safety acceptance specifications, the safety improvement of the 3-valve FB system is significant.

A formal cost/risk-benefit analysis can then be conducted to determine whether the cost trade-off justifies the addition of the third EM valve to the original FB system.

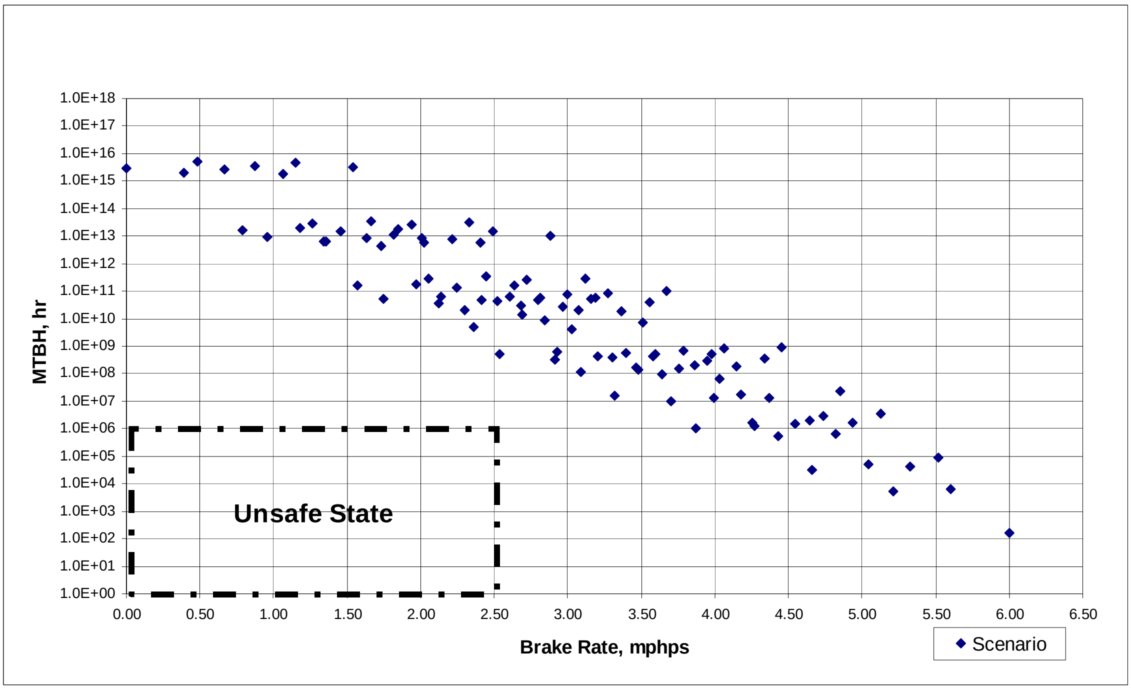


Figure 6 - The Risk Profile of the Accident Scenarios in Example 2

The 3-valve system would also allow a higher GEBR for a greater throughput; however, the brake rate achieved is limited by the available wheel/rail adhesion. The assumed 16% adhesion in Example 1 can only support an effective brake rate as high as approximately 3.2 mphps (μ•g). Any higher brake rate may cause wheel slide, thus, the system safety is compromised.

CONCLUSIONS

The paper uses the above practical examples to illustrate the proper use of integrated fault tree/event tree techniques in a QRA process. The above techniques can also apply to other meaningful applications.

Compare Similar Design Options

The model can be used to compare similar design options in terms of their risk impact. Traditional worst-case analysis and the MIL-STD-882 type analysis generally cannot distinguish between alternative designs that are very similar in both likelihood and severity impacts. The fault tree structure can determine the overall risk impact to a system at the component level. Once the risk is known, a formal cost/risk-benefit analysis can then be performed to select the optimal design.

Identify Total Risk

It would be advantageous to a transit system to develop a comprehensive risk model that encompasses all aspects of the system. Once the total risk of the system is assessed, a cost/risk-benefit analysis can be performed to mitigate or eliminate the dominant risk contributors.

Another typical use of the model is to optimize the maintenance interval. The model can be used to determine an optimal maintenance and inspection interval. Most of the maintenance and inspection schedules developed to date are based on past experience and industry standards. For an advanced system, the schedule should be based on the actual performance of the system instead of a prescriptive industry standard. A comprehensive risk model allows the users to assess the risk impact to the system with different maintenance and inspection intervals. The interval that results in the least total risk impact would be the ideal maintenance interval.

There can be many potential applications for the risk-based approach is applied properly in analyzing the performance of a transit system. The model can help transit management identify dominant risk contributors, enhance safety, and improve throughput.

REFERENCES

1. Reactor Safety Study, Wash-1400, U.S. Nuclear Regulatory Commission, 1975.