The Value of Graphical Models for Quantifying Risk

Paul Britton (NASA) and Will Janzer (Bastion)

paul.t.britton@nasa.gov

william.o.Janzer@nasa.gov

Table of Contents

Background and History

- Block diagrams were introduced in the early 1920s at an ASME conference
- These methods of problem analysis would begin seeing use in industry in the 30s and 40s
- In 1947 ASME released *Operation and Flow Process Charts* standardizing the symbols required in these diagrams
- These methods evolved into block diagrams as we know them today and eventually fault trees
- In the 1960 the Nuclear industry began applying Probabilistic Risk Assessment to their plants in a similar way to how we use it today

General Benefits

- Facilitate design influence at lower levels and make risk informed decisions prior to your mission
- Quantify risk with no top-level data
- Eliminate inefficient serial process flows from risk analysis via collaborative development and division of labor
- Useful way to communicate risk to others who might not be as well versed in the way risk is mapped and calculated
- Shows others how you are using their data (e.g. software, part reliability, structures etc.) in calculating risk to support a more transparent risk management approach

Definitions

- **Reliability** is the probability that component or system will perform its intended function adequately for a specified duration in a specified environment
- **Unreliability** or **Failure Probability** is the probability that component or system ***fails*** to perform its intended function adequately for a specified duration in a specified environment
- **Notational Conventions**
  - The reliability of components 1 and 2 are called R1 and R2
  - The failure probabilities of components 1 and 2 are called Q1 and Q2
  - The reliability and unreliability of a system are called Rs and Qs
- **Basic result:** From the Axioms of a Probability Space, R + Q = 1

Algebraic Calculation of Risk

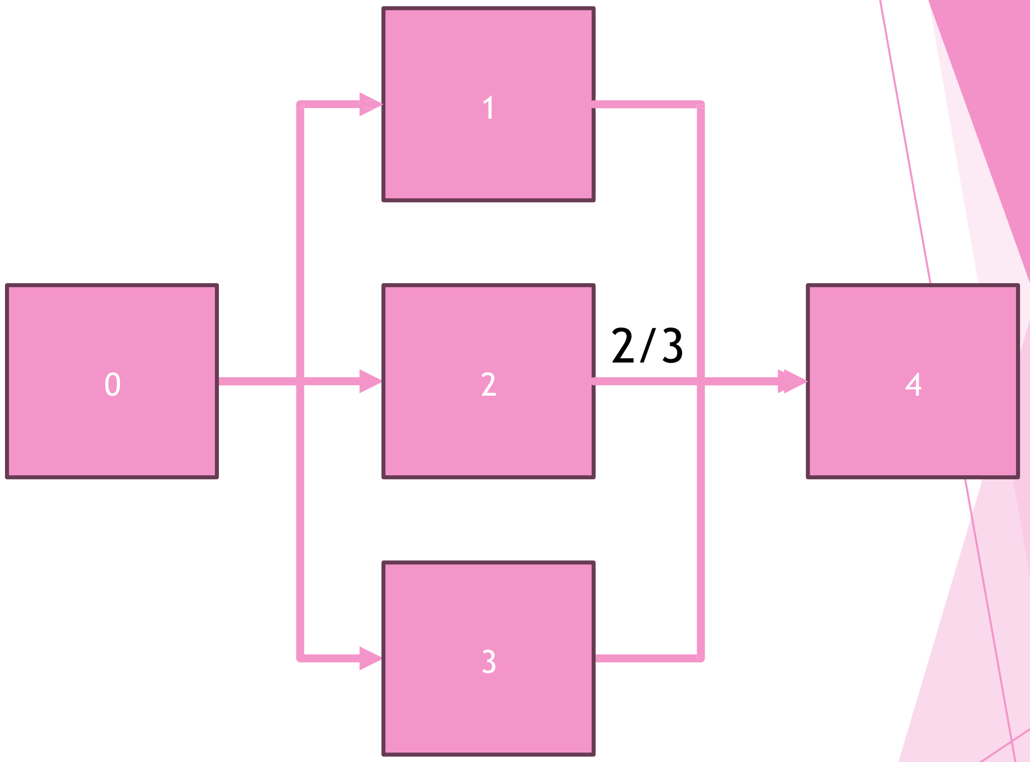
- Reliability and Unreliability of two component systems
  - Series Reliability / Risk Or-gate / 2 of 2 Success Criteria
    - Rs = R1*R2
  - Parallel Reliability / Risk And-gate / 1 of 2 Success Criteria
    - Qs = Q1*Q2
- System Failure Probability of like component redundant systems (with M of N Success Criteria)
  - $Q_s = \sum_{k=0}^{M-1} \binom{N}{k} R^k Q^{(N-k)}$
- **System Equations**
  - **System Reliability:** An equation for Rs that is consistent with the failure logic of the system that is derived from system objectives and design schematics
  - **System Failure Probability:** An equation for Qs that is consistent with the failure logic of the system that is derived from system objectives and design schematics
  - System Equations are derived with the aid of Graphical Models

The Fundamentals of Various Graphical Representations of Risk

- Reliability Block Diagrams
- Event Sequence Diagrams
- Event Trees
- Fault Trees
- Bayesian Networks
- Influence Diagrams

Reliability Block Diagrams

- Reliability Block Diagrams depict component reliability and redundancy relationships throughout and with a system
- Their main use is to aid with computing system reliability

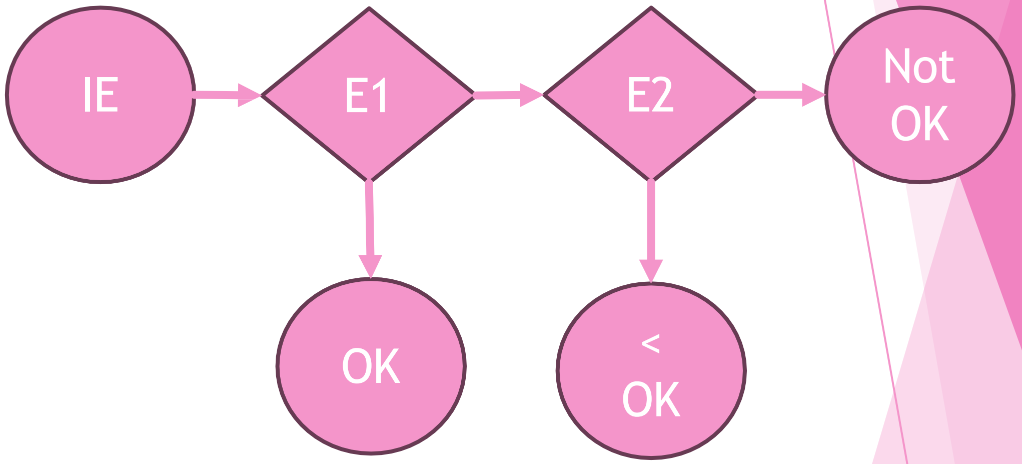


Rs = R0 * R2/3 * R4 = R0 * (Q1^3 + 3*R1*Q1^2) * R4

assuming components 1, 2, and 3 are like components

Event Sequence Diagram (ESD)

- Bottom-up approach
- “Yes” will always lead right and “No” will always lead down
- ESDs represent a chain of Boolean Events or even a tree of Boolean Events
- The initiating event and end states are circles, and the pivotal events are diamonds
- In this example:
  - IE = Drive to Store
  - E1 = Wreck Given IE
  - E2 = Air Bag Fails Given E1
  - P(OK) + P(< OK) + P(Not OK) = 1
- ESDs are simple yet flexible since they allow multiple end states



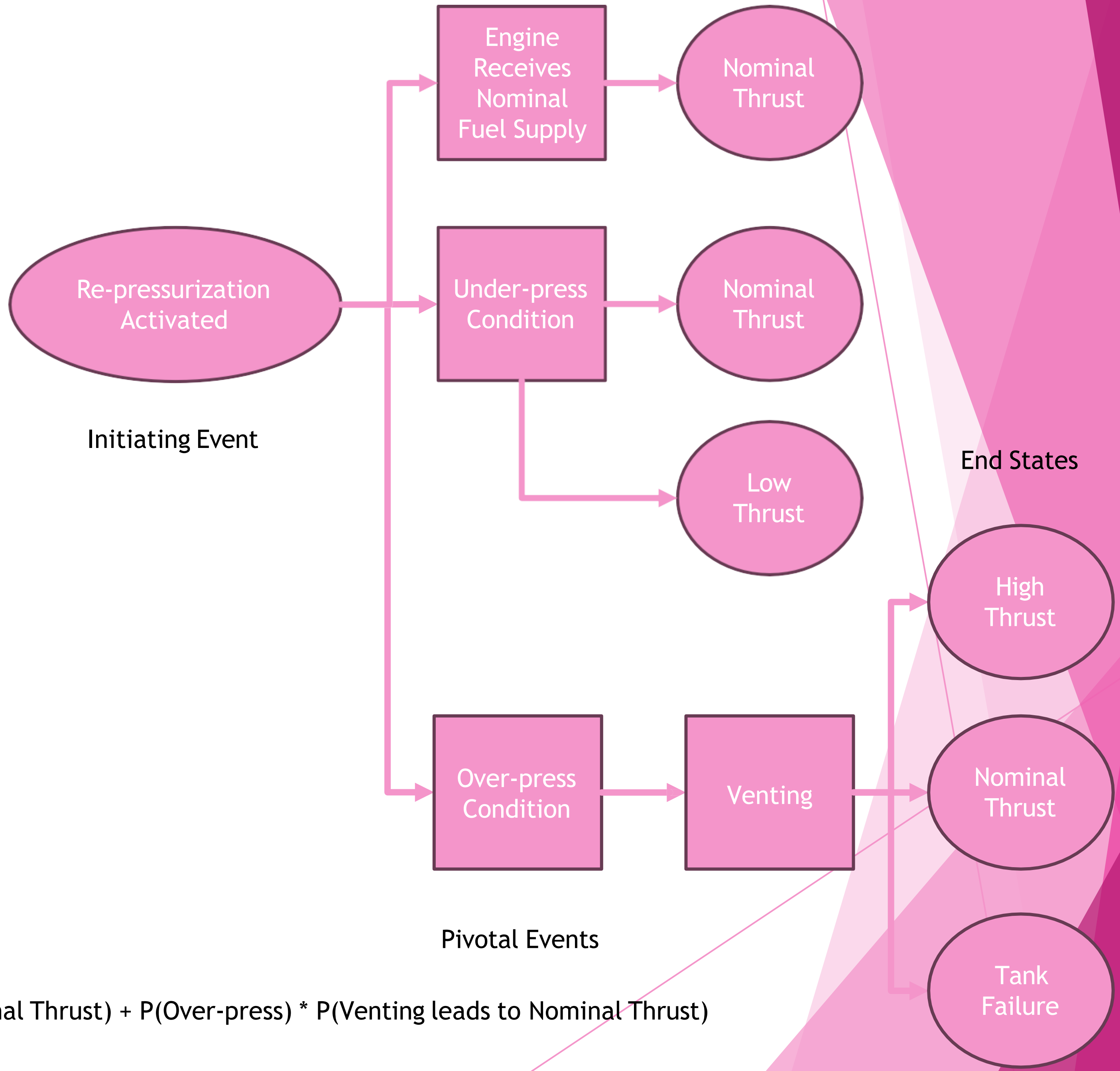
P(OK) = 1 – E1

P(< OK) = E1 * (1 – E2)

P(Not OK) = E1 * E2

Event Trees

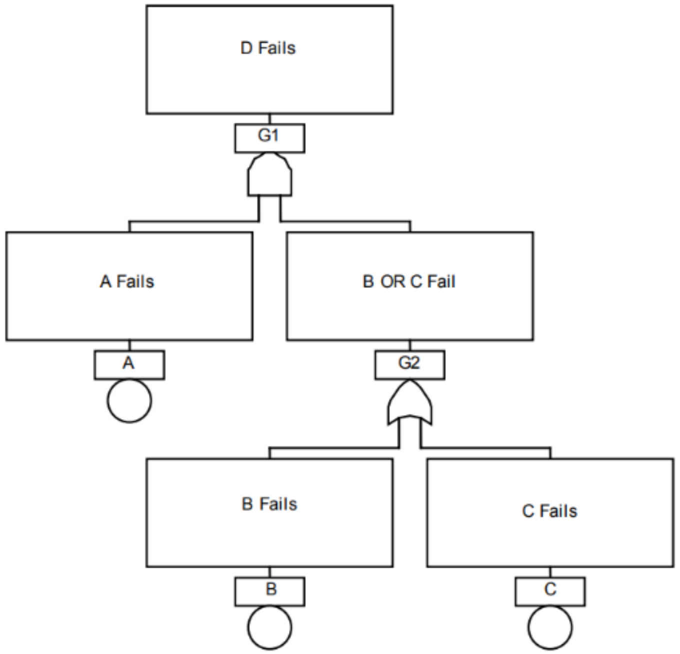
- Event Trees are an extension of ESDs
- Formally, ESDs are binary trees whereas Event Trees are N-ary trees
- Event Trees are not restricted to Yes/No events although some Event Trees are formulated with binary branching
- Pivotal events can have multiple outcomes, but the outcomes must be mutually exclusive (i.e. they are Categorical rather than just Boolean)
- The probability of achieving a specific end state given the initiating event is computed as a sum-product of the branches leading to that end state
- Event Trees model all possible pathways within the scope



P(Nominal Thrust) = P(Under-press leads to Nominal Thrust) + P(Over-press) * P(Venting leads to Nominal Thrust)

Fault Trees

- Top-down approach. End event is undesired with sub events being failures that lead there.
- Gates are used to represent Boolean logic
- And = 
- Or = 
- Not, XOR and M/N Gates are also used
- Each basic event (circles) has an associated failure rate or failure probability
- You can solve any individual gate for the failure probability of that specific part of the system
- Allows easy integration of uncertainty calculations to impact results in an informative way.
- Fault Trees are useful throughout the design process



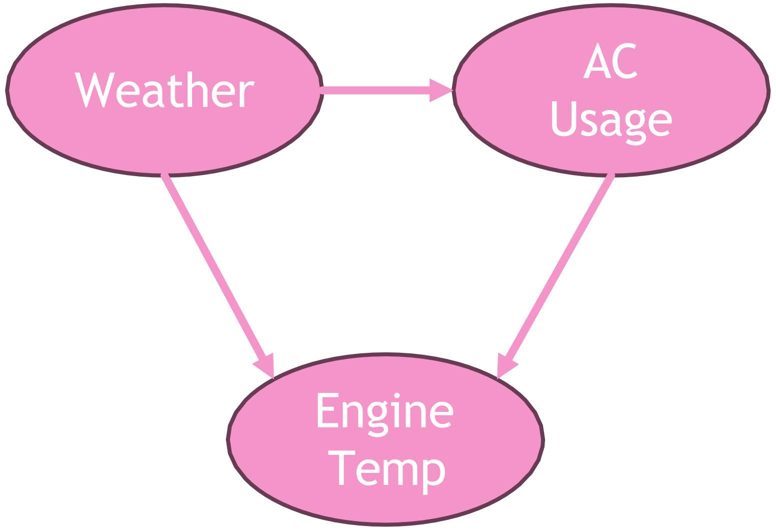
$Qd = Qa * (1 - Rb*Rc)$

Bayesian Networks

- Probabilistic model depicting random variables and their conditional dependencies
- Mathematically they are directed acyclic graphs
- A pair of nodes where there is no path connecting them are conditionally independent
- Note: In this example, all three variables are Boolean, but they can be discrete or continuous variables

Above 90˚F	
T	F
0.7	0.3

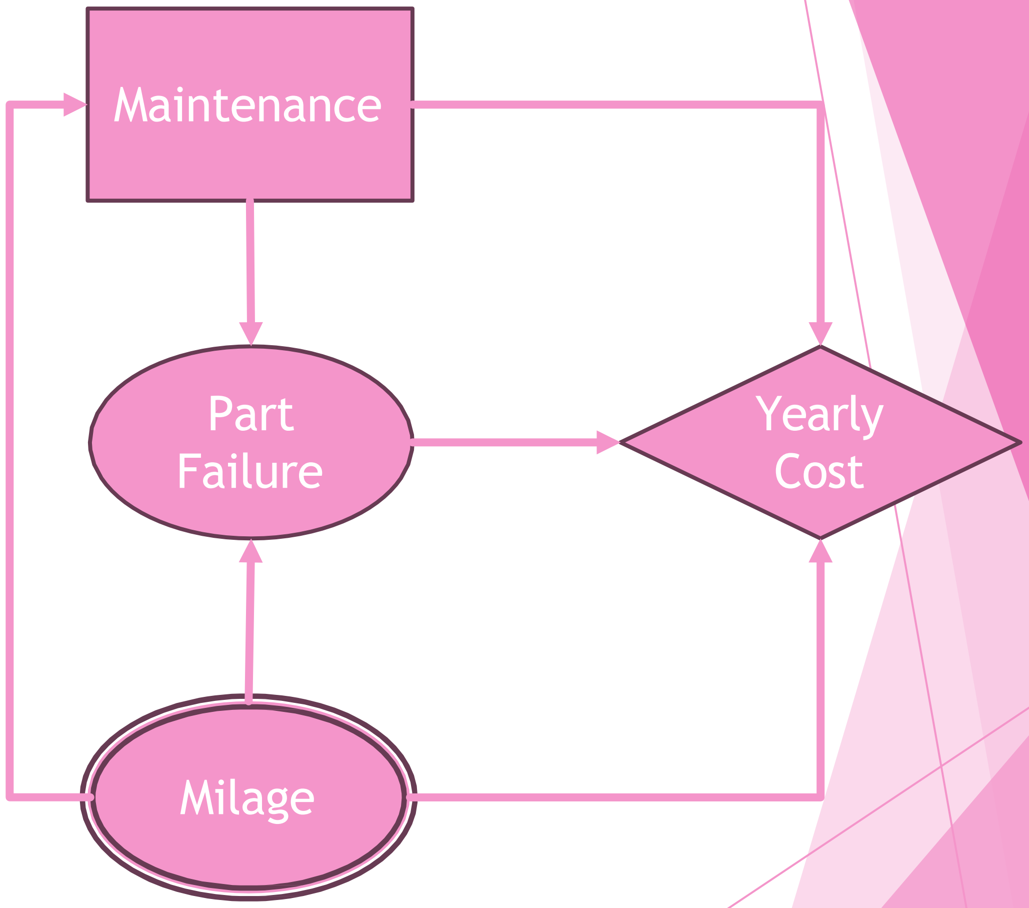
Above 90˚F	AC On	
	T	F
T	0.5	0.2
F	0.2	0.1



Above 90˚F	AC On	Engine Redline	
		T	F
T	T	0.3	0.2
T	F	0.15	0.05
F	T	0.15	0.05
F	F	0.06	0.04

Influence Diagrams

- Mathematically, influence diagrams are also directed acyclic graphs
- Four main node types:
  - Ovals are uncertain
  - Double ovals are deterministic
  - Rectangles are decisions
  - Diamonds are output values
- Decision nodes represent control variables that can be adjusted to affect the output values
- Once programmed into a spreadsheet or script language, algorithms like Newtons Method can be used to optimize the output values



Summary

- Graphical quantifications of risk are a developmental tool that create and encourage a deeper understanding of a systems risk prior to having any hard test data on the system or its components
- They can and should be used throughout the design process to assess and communicate system risk
- Risk models get more accurate and more complex as a system goes through its design process which is why graphical representation can be beneficial for communication

Source links

- nasa.sharepoint.com/teams/HLSSMARMPRA/Shared Documents/Forms/AllItems.aspx?id=%2Fteams%2FHLSSMARMPRA%2FShared Documents%2FTraining%2FPRA Guide_NASA%2Epdf&parent=%2Fteams%2FHLSSMARMPRA%2FShared Documents%2FTraining
- NUREG-0492, "Fault Tree Handbook". (nrc.gov)
- #1 - ASME standard; operation and flow process charts, 1947 - Full View | HathiTrust Digital Library
- NUREG/KM-0010, "WASH-1400 - The Reactor Safety Study - The Introduction of Risk Assessment to the Regulation of Nuclear Reactors." (nrc.gov)
- Boolean algebra - Wikipedia
- Flowchart - Wikipedia

Backup

Basic Risk Modeling Concepts

- Boolean Algebra
  - Most graphical models are just visual ways of presenting Boolean algebra. Simple Boolean algebra, for our purposes, is AND and OR.
    - AND
      - Notation: $x \wedge y$
      - Definition: $x \wedge y = 1$ if $x = y = 1, x \wedge y = 0$ otherwise
      - Multiplication
    - OR
      - Notation: $x \vee y$
      - Definition: $x \vee y = 0$ if $x = y = 0, x \vee y = 1$ otherwise
      - Addition
- Cutsets
  - The divisions of events in sequence that result in the undesired end state.