



Center for Air Transportation Systems Research (CATSR)

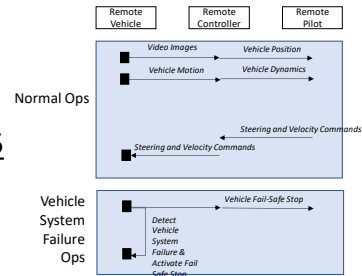
Accounting for Uncertainty in Safety & Reliability of AI-enabled Systems

▶ Lance Sherry, John Shortle, Matthew Amissah, Ali Raz

June 9, 2026

System Engineering and System Safety Artifacts

Con-Ops



Mission Requirement

RPR Mission Requirements

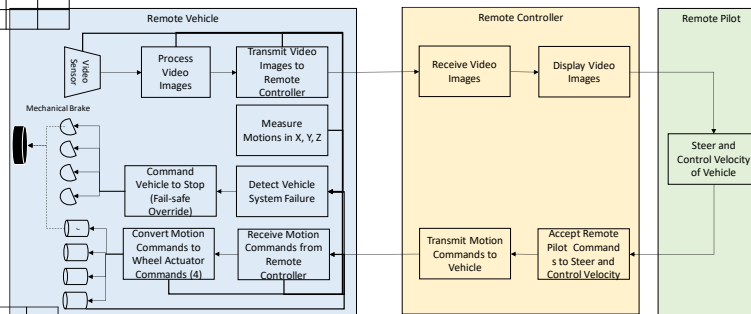
....

MR: n The RPR System (vehicle + controller + operator) shall not exceed a fatality, injury, or property damage rate of 10E-3

Req to Functions Traceability Matrix

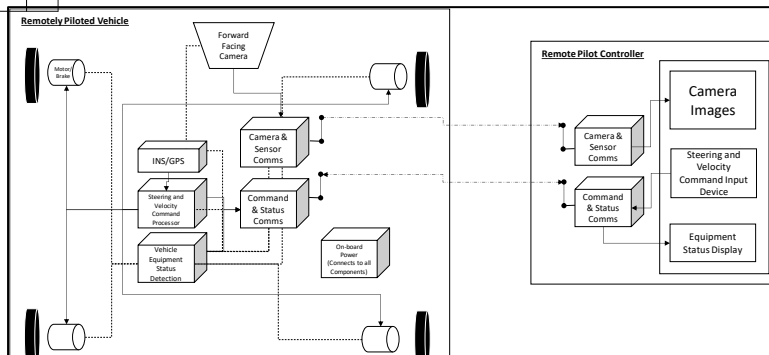
				

Functional/ Logical Model



Functions to Components Traceability Matrix

Component/ Physical Model

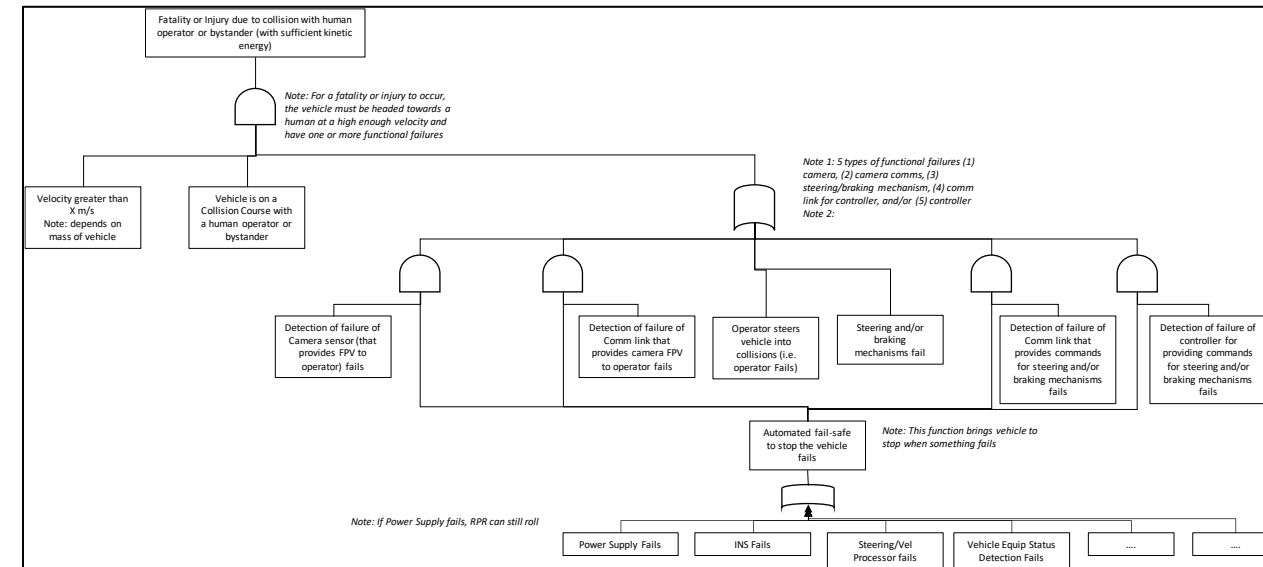


Hazard Analysis

RPR Hazards

- ...
- ...
- Collide with bystander causing fatality or injury
- Collide with operator causing fatality or injury
- Collide with infrastructure causing property damage
- ...

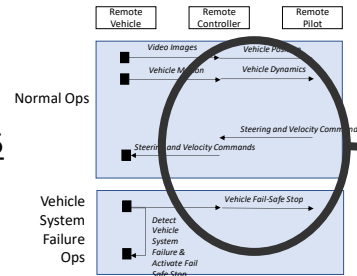
Safety Model



System Engineering and System Safety Artifacts

Hazard Analysis

Con-Ops



RPR Hazards

- ...
- ...
- Collide with bystander causing fatality or injury
- Collide with operator causing fatality or injury
- Collide with infrastructure causing property damage
- ...

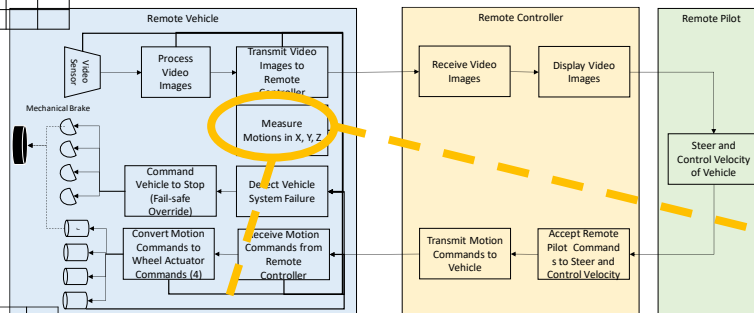
Mission Requirement

RPR Mission Requirements

MR: n The RPR System (vehicle + controller + operator) shall not exceed a fatality, injury, or property damage rate of $10E-3$

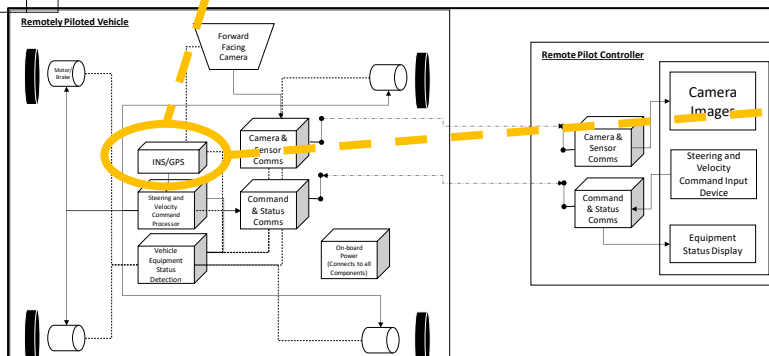
Req to Functions Traceability Matrix

Functional/Logical Model

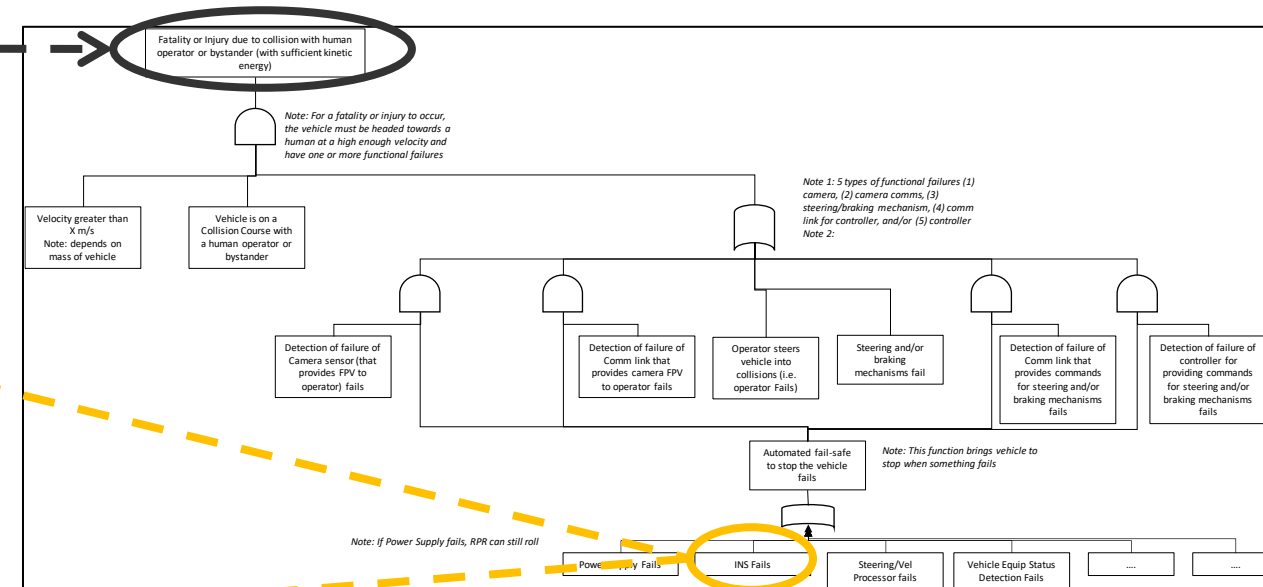


Functions to Components Traceability Matrix

Component/Physical Model



Safety Model



Motivation

- AI-enabled systems are increasingly autonomous and distributed
- Traditional SSA assumes largely deterministic behavior
- AI introduces probabilistic, adaptive, and data-dependent behavior
- Need explicit treatment of uncertainty

Sources of Uncertainty

1. Training data limitations and bias
2. Model generalization errors
3. Distribution shifts and changing environments
4. Sensor inaccuracies and human-AI interaction
5. Emergent behaviors not observed during development

Types of Uncertainty

- Aleatory: inherent variability in operations
- Epistemic: lack of knowledge about system behavior
- Both affect safety and reliability estimates
- Must be represented explicitly in assurance activities

Uncertainty Quantification (UQ)

- Quantifies confidence in safety assessments
- Evaluates uncertainty in data, assumptions, and predictions
- Supports transparent risk-informed decisions
- Especially valuable in early design phases

Methods for UQ

- Probabilistic Risk Assessment (PRA)
- Bayesian inference and Bayesian networks
- Monte Carlo simulation
- Sensitivity analysis
- Confidence interval estimation

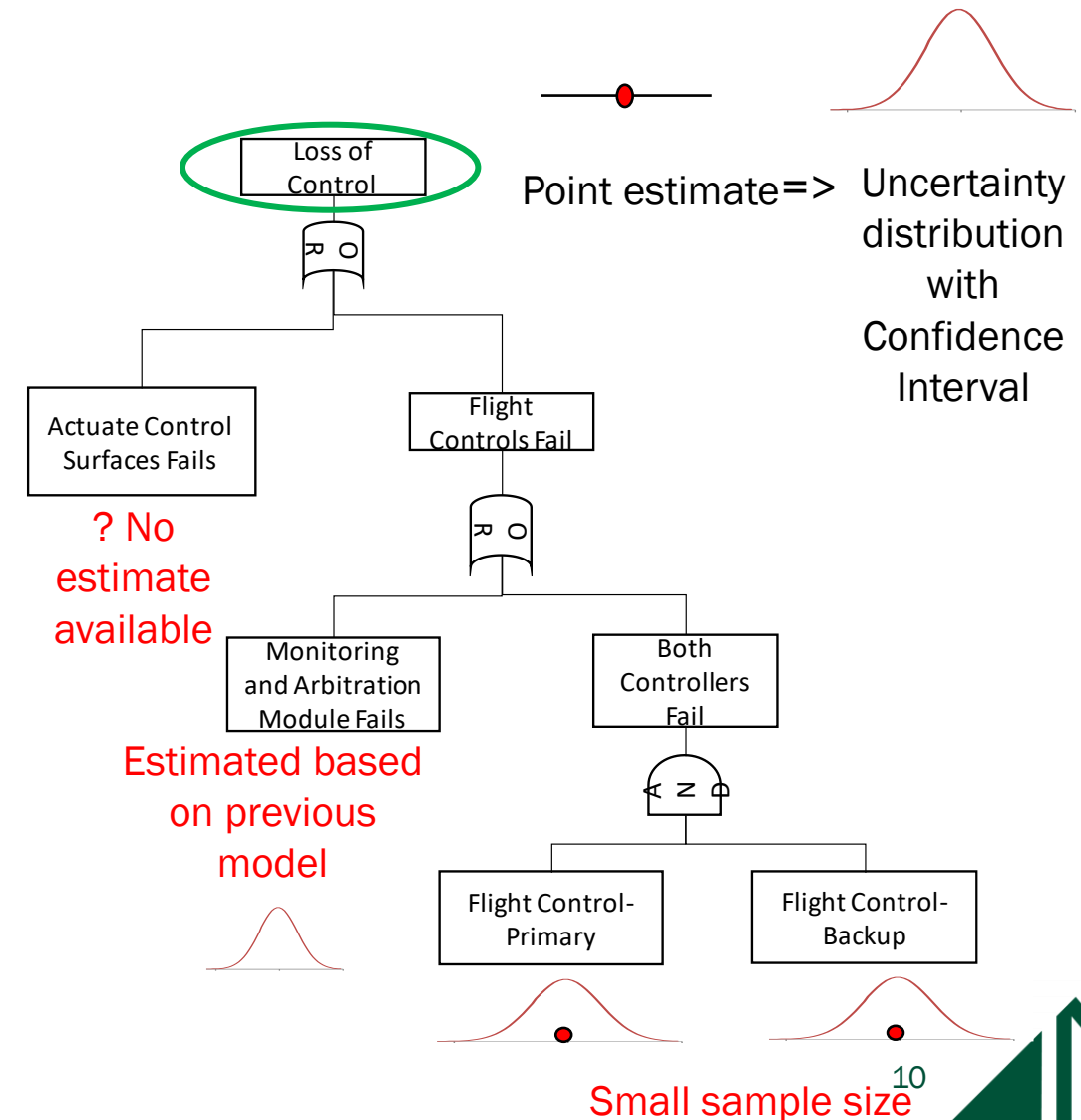
Fault Tree Analysis for AI Systems

- Traditional FTA uses fixed failure probabilities
- AI behavior violates deterministic assumptions
- Represent basic events with distributions rather than point estimates
- Propagate uncertainty to top-event risk

Fault Tree Uncertainty Analysis

Design Challenges

- AI-based systems: Incomplete or biased training data; model drift; changing operational environments
- FT parameters may be rare events, resulting in noisy point estimates
- Some FT parameters may have no supporting data for quantification

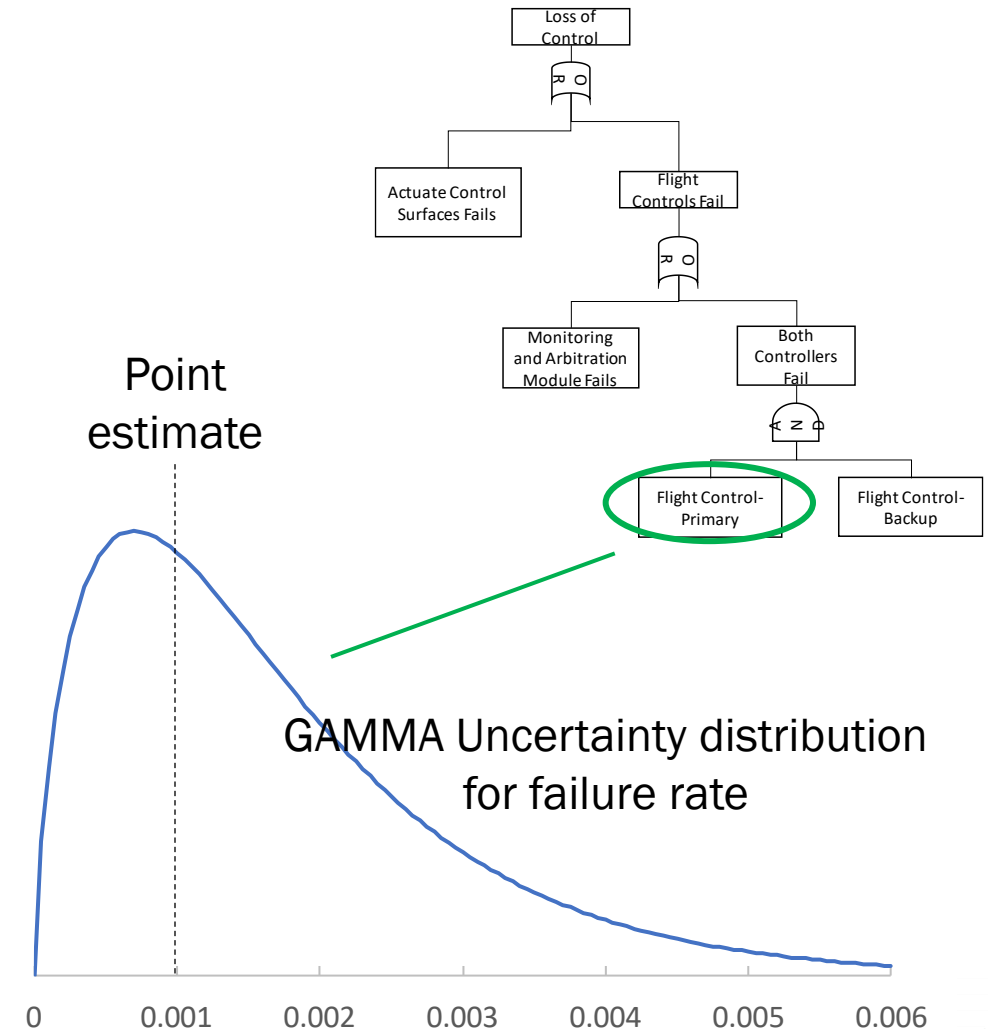


Potential Sources of Uncertainty

- Rare-event data: E.g., if 1 event is observed out of N operations, upper bound for true probability is $5.57 / N$ (95% confidence interval)
- Unquantified: Events with no supporting data
- Expert judgment
- Non-representative data: E.g., drift of AI model
- Measurement error: Errors in collecting data (e.g., LLM analysis of textual incident reports)

Replace Point Estimates with Distributions

- Suppose 1 failure is observed in 1,000 hours of testing for primary flight controller
 - The point estimate for the failure rate is $1\text{E-}3$
 - Based on the point estimate, the uncertainty distribution for the failure rate is a gamma distribution with parameters $\alpha = 1.5$, $\beta = 1,000$
- General method: If k failures observed from n trials, assign uncertainty distribution for failure probability as a gamma distribution with parameters $\alpha = 0.5 + k$, $\beta = n$
- Approach based on Bayesian updating of Poisson distribution



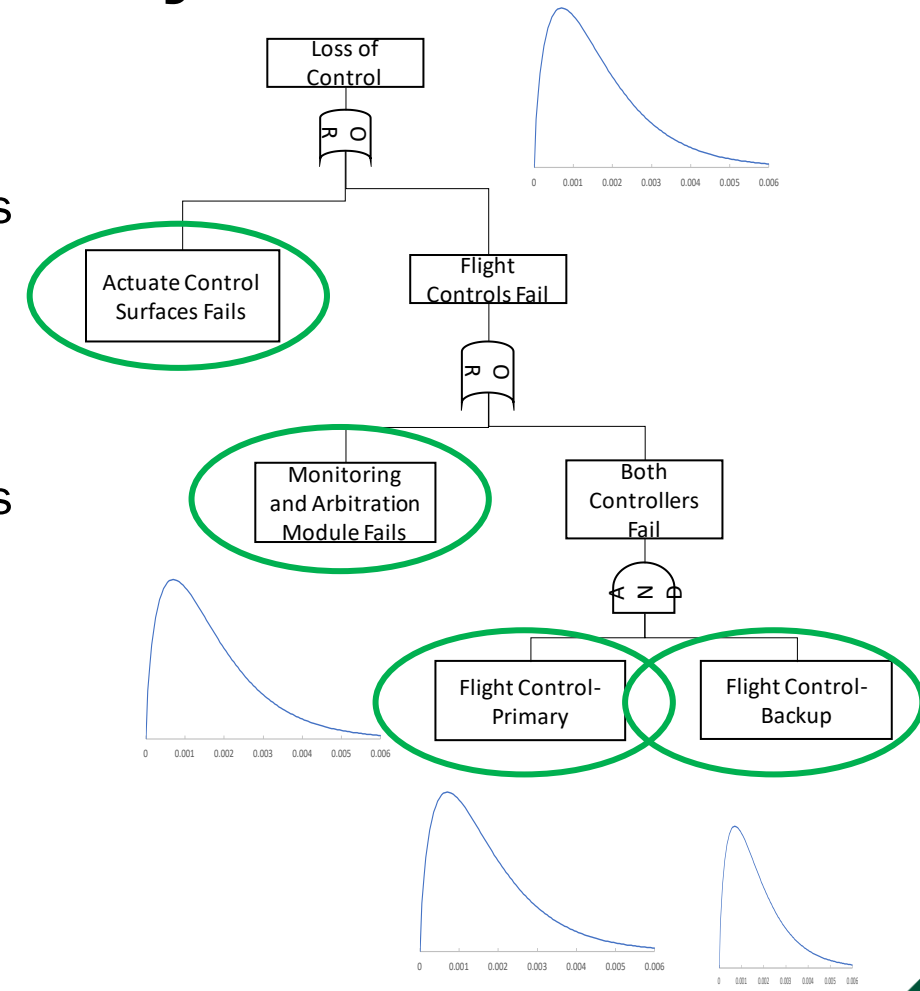
Calculating Top-Level Uncertainty

Standard approach

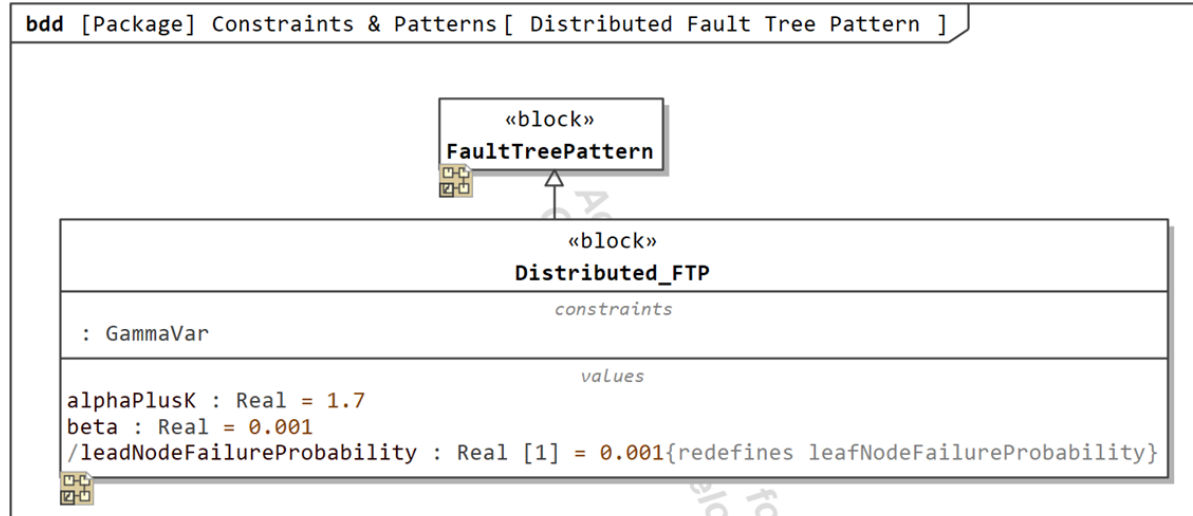
- Measure failure probability of each base event (e.g., k failures out of n trials)
- Quantify each base event with its point estimate (e.g., k/n)
- Quantify fault tree from bottom-up using AND/OR gate logic

Uncertainty approach

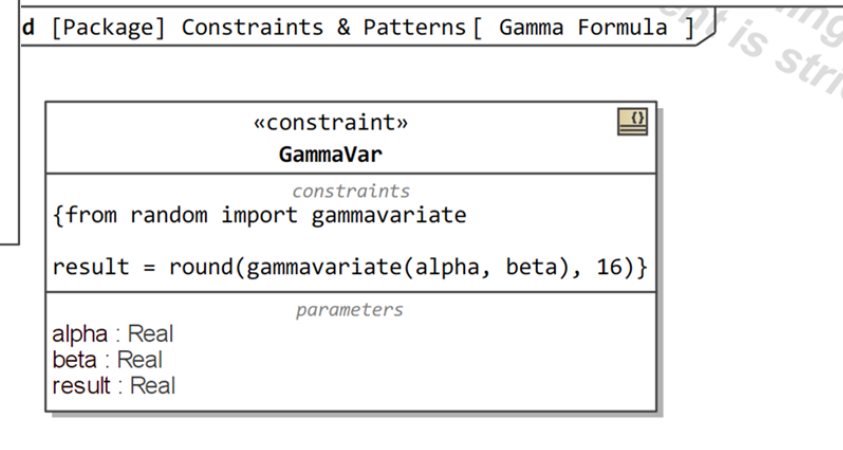
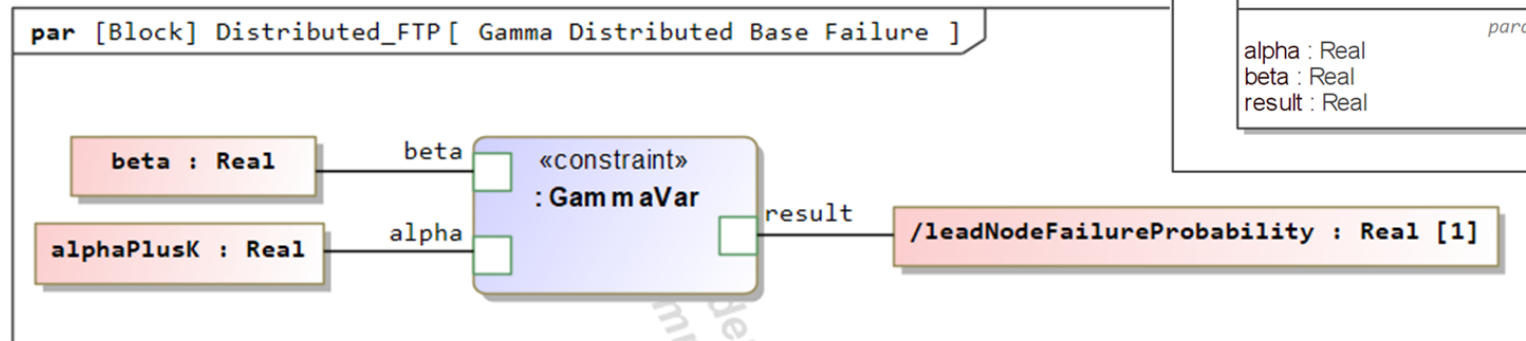
- Measure failure probability of each base event (e.g., k failures out of n trials)
- Assign each base event an uncertainty distribution (gamma distribution with $\alpha = 0.5 + k$, $\beta = n$)
- Monte Carlo simulation loop:
 - For each base event, take a random draw its uncertainty distribution
 - Quantify the fault tree from bottom-up with AND/OR logic
- Assemble distribution of top-level event and any other events of interest



Implementation in SysML



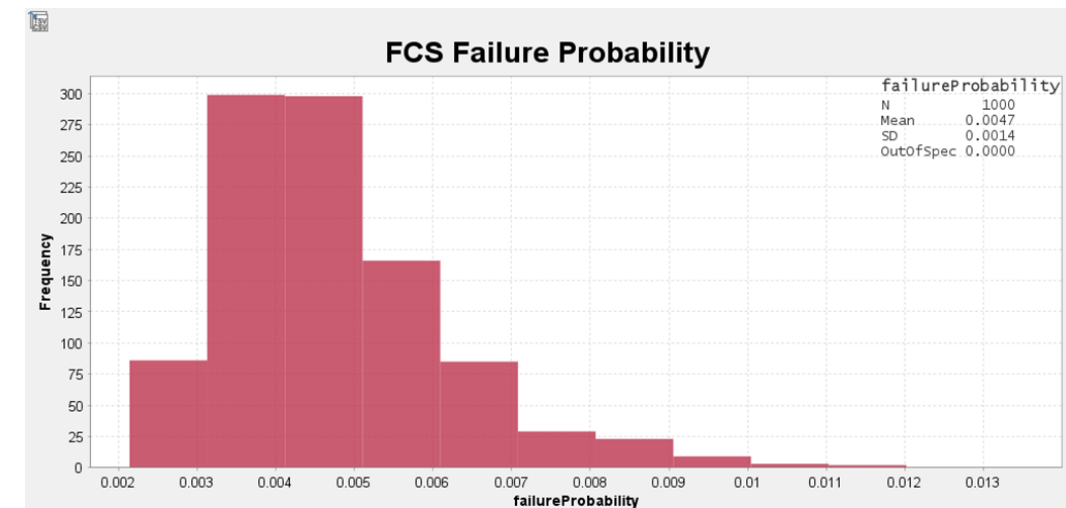
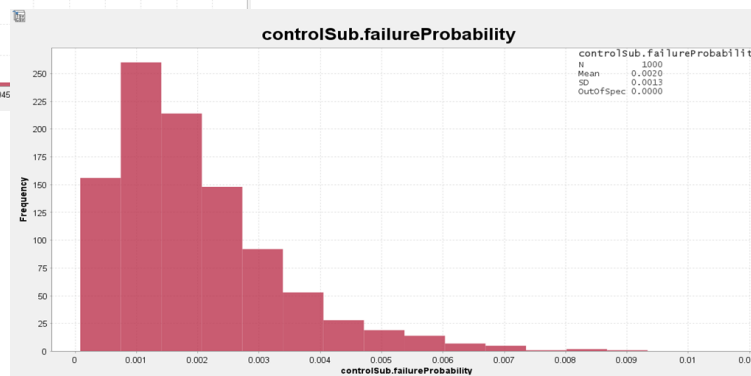
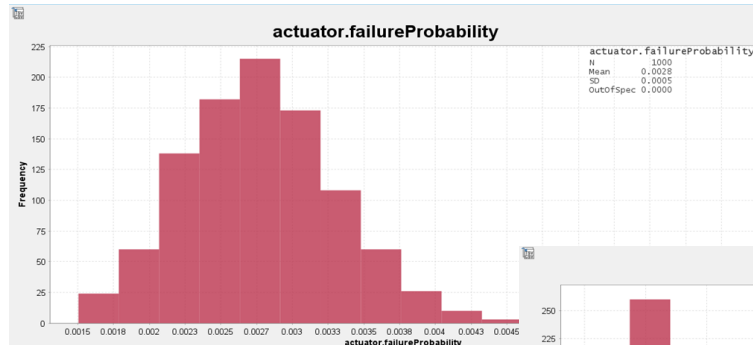
- Leaf node probability is defined a gamma random variable



Uncertainty Implementation in SysML

Monte-Carlo Simulation Initial Values

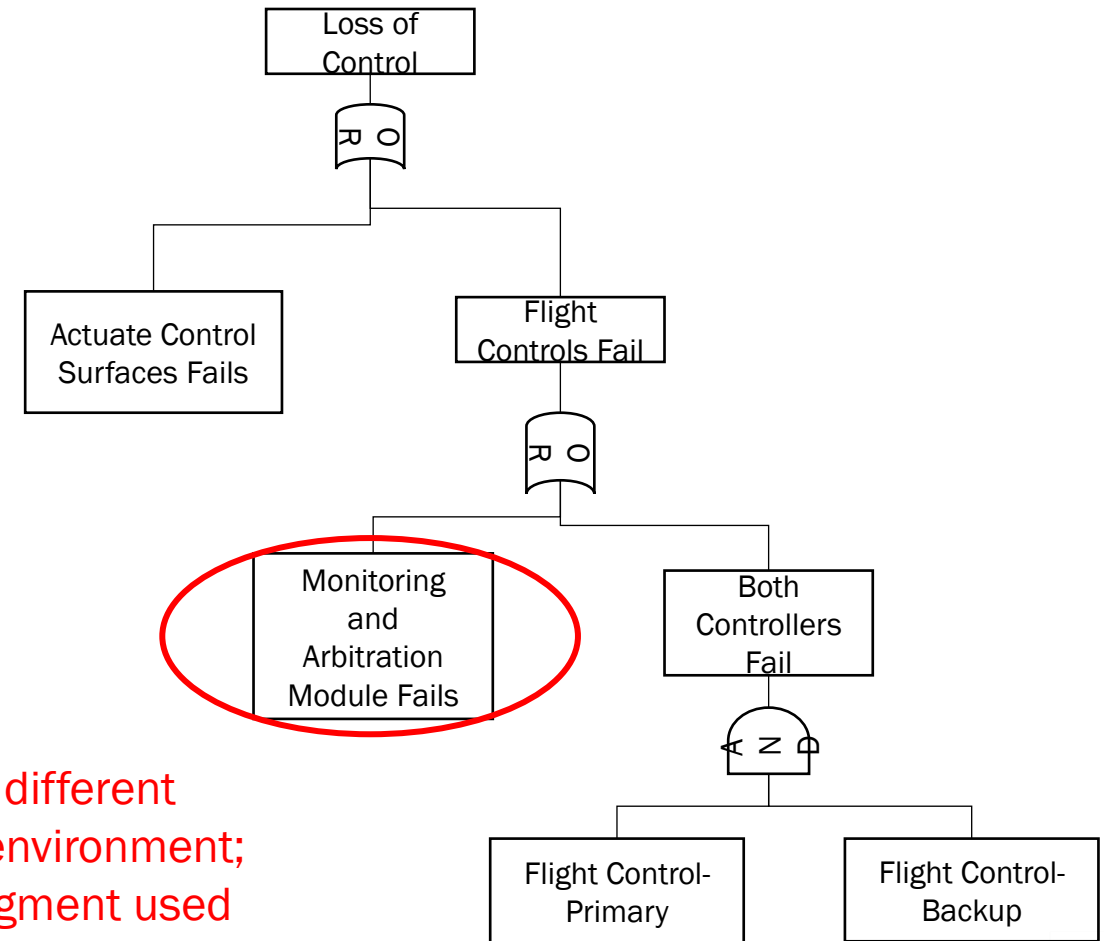
#	Name	 beta	 alphaPlusK	 leadNodeFailur...	 failureProbability	 orSubs	 andSubs
1	 flightControlSystem	1.0E-12	1	4.0E-12	0.0035	 controlSub : Struct  actuator : Structur	
2	 actuator	0.0001	27.5	0.0017	0.0017		
3	 controlSub	1.0E-12	1	1.0E-12	0.0018	 mAndA : Structure	 primaryCtrl  backupCtrl
4	 primaryCtrl	0.005	3.5	0.0118	0.0118		
5	 backupCtrl	0.0175	1.5	0.0372	0.0372		
6	 mAndA	0.001	1.5	0.0014	0.0014		



Interval Analysis

Design Challenge:

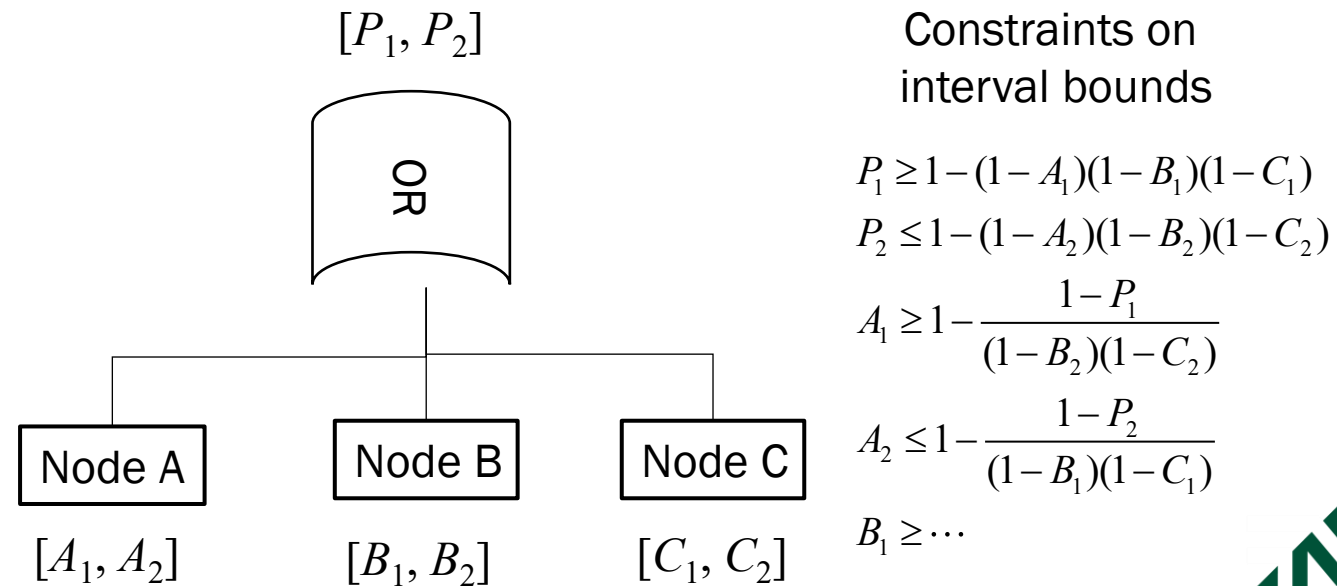
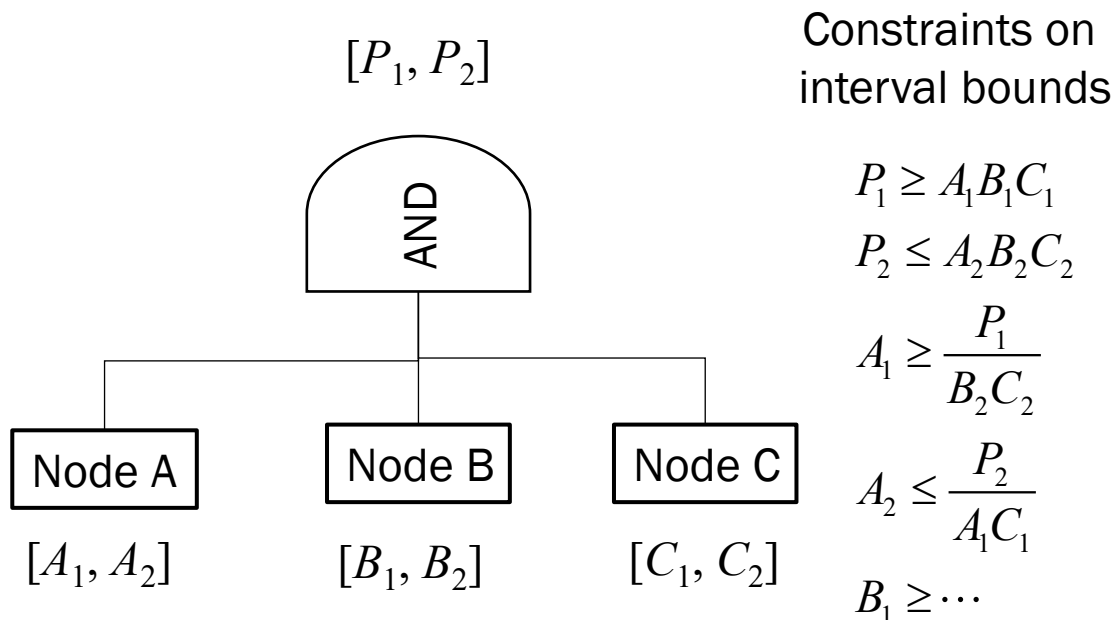
- What is risk budget assigned to (new) function to meet top-level risk
 - What are implications for ranges of other nodes in the tree?
 - How do constraints on top level probabilities flow down to requirements on base events?



Data in different
operating environment;
expert judgment used
to map failure rates
from test environment

Interval Analysis, Theory

- Each node is quantified by a lower bound and upper bound on the event probability
 - If the event probability is known exactly, lower bound = upper bound
 - If the event probability is unknown, its probability interval is $[0, 1]$
- Intervals can be narrowed based on constraints between children and parents

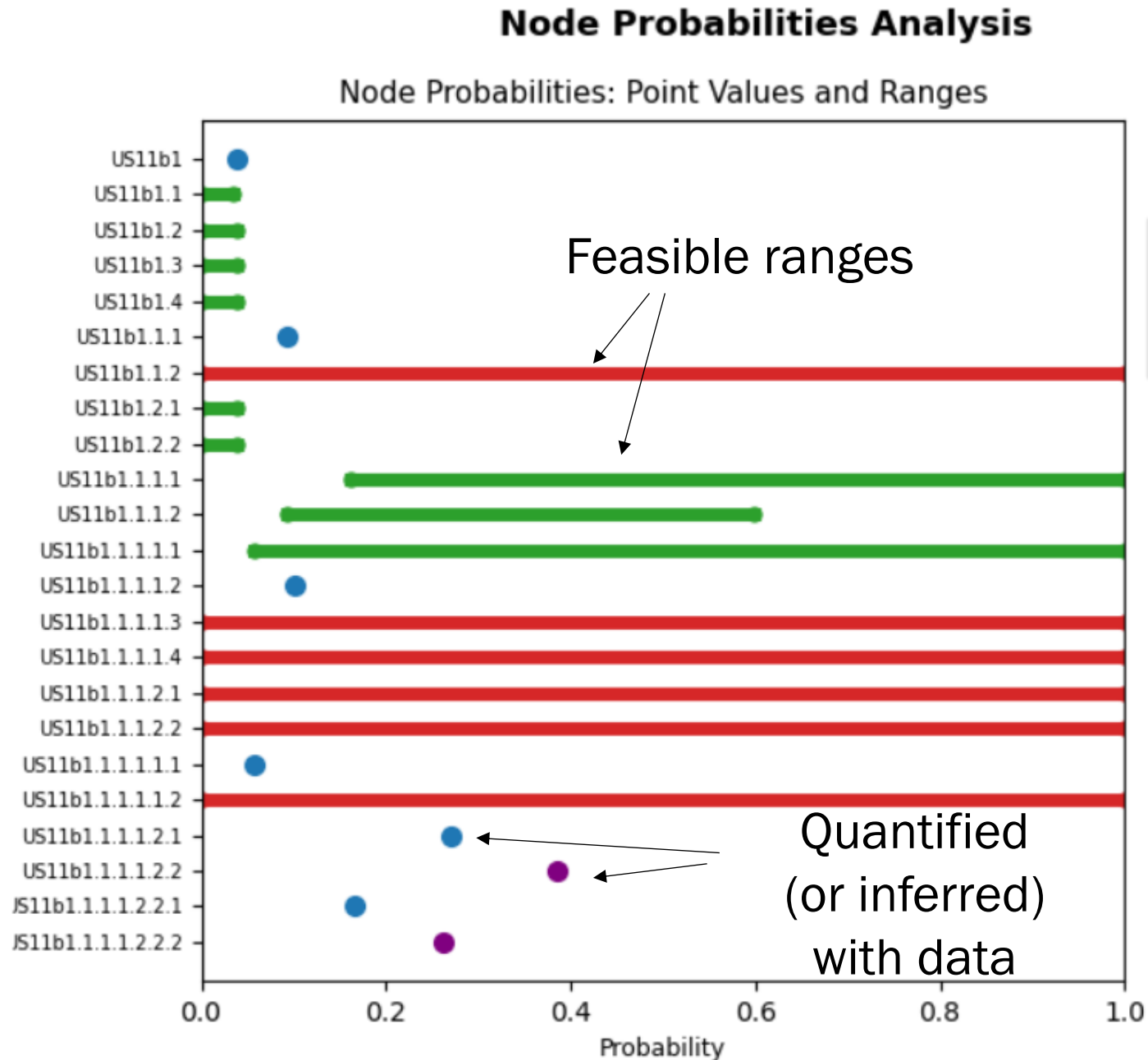
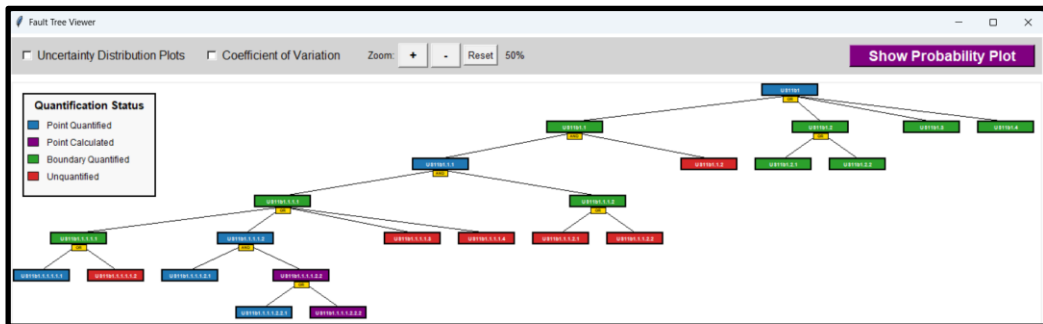


Interval Analysis Algorithm

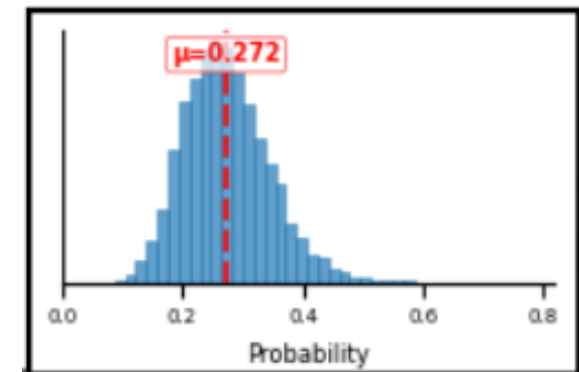
- Initialization intervals:
 - Quantified nodes: $[p_i, p_i]$ (interval with zero width)
 - Unquantified nodes: $[0, 1]$
 - Expert judgment: $[a_i, b_i]$, where $a_i < b_i$
- Iterative step: Cycle through each node of the tree
 - Forward pass: Parent nodes updated based on children
 - Backward pass: Child nodes updated based on parent and siblings
 - Intervals remain the same or tighten
- Stop when no change in intervals

Interval Analysis

- Identifies which nodes can be quantified or calculated from point estimates
- For other nodes, shows feasible range of values



- Generate and display uncertainty distributions for each node



Benefits of UQ-Enhanced FTA

- Distribution of possible top-event probabilities
- Confidence bounds on risk estimates
- Identification of dominant uncertainty drivers
- Supports certification and assurance arguments

Assurance for AI-enabled Systems

- Assurance cases and claims-based evidence
- Formal verification and robustness testing
- Adversarial evaluation
- Operational monitoring and human oversight
- Focus on acceptable residual risk

Key Takeaways

- Deterministic certification is evolving to evidence-based assurance
- Uncertainty must be quantified and bounded
- UQ strengthens SSA for AI-enabled systems
- Critical for transportation, healthcare, defense, and automation

Summary

- Integration of methods for uncertainty analysis in system safety (interval analysis, stochastic uncertainty, expert judgment, ...)
- Implementation of methods in SysML and other tools
- Potential use cases
 - Flow of safety requirements to components, accounting for uncertainty
 - Quantify value of data in demonstrating system meets target level of safety

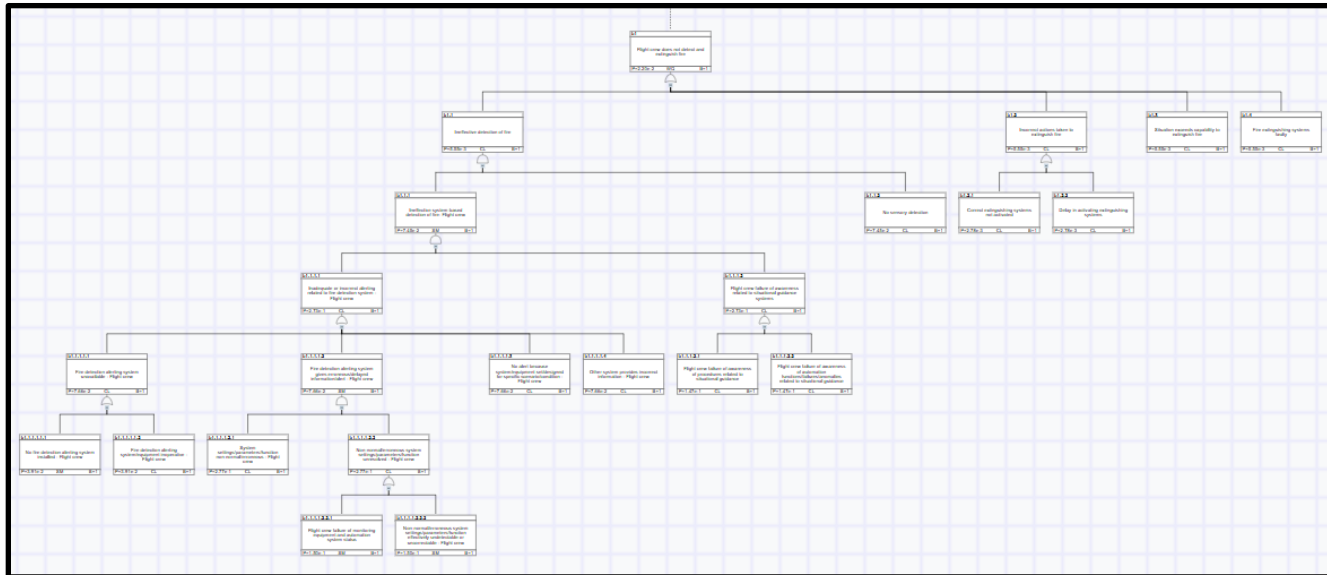


Backup



System Safety Uncertainty Analysis

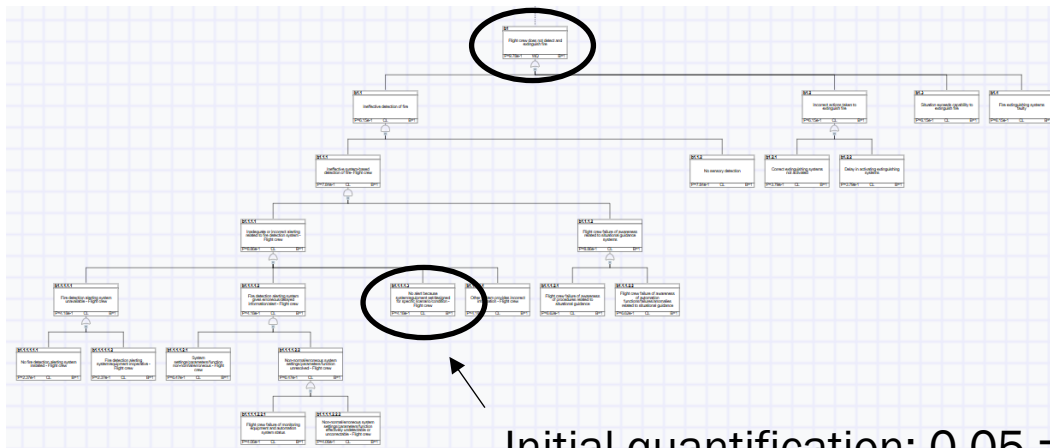
- Motivation: In safety-critical applications, where events are rare and data are limited or missing, it is important to quantify both a predicted value and its associated uncertainty



Target Level of Safety with Uncertainty

Question	Methodology	Without Uncertainty	With Uncertainty
What will further data collection reveal about system safety?	Node is initially quantified with limited data (e.g., 5 out of 100); more observations are obtained (e.g., 47 out of 1,000). Re-quantify tree with new data set	Observe change in top-level probability (likely a small change)	Observe change in <u>95% upper bound</u> of top-level probability – may change significantly

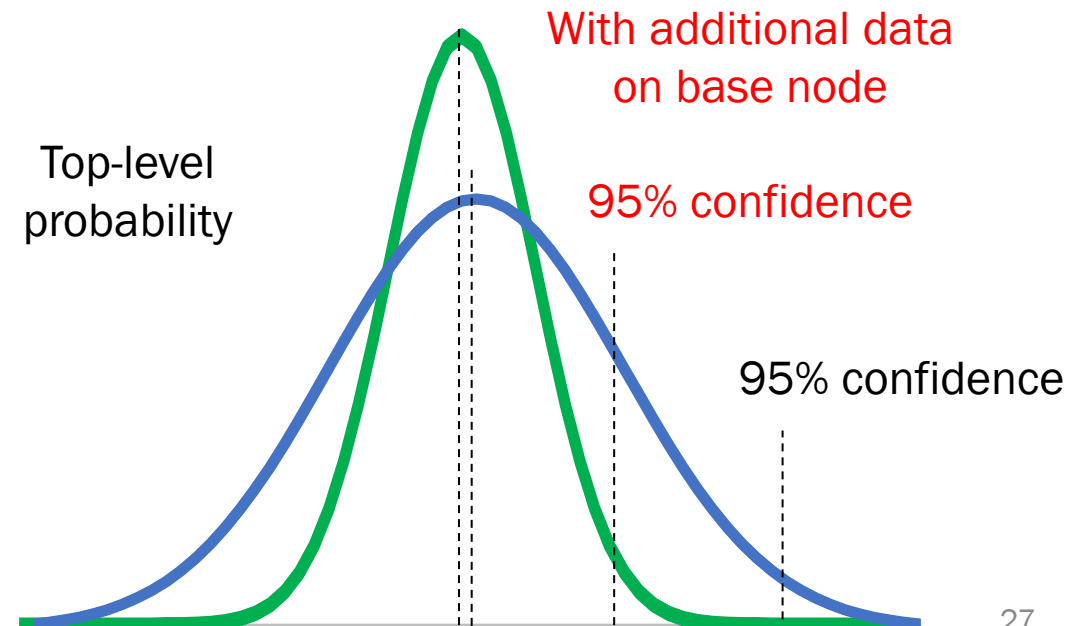
Using Point Estimates



Initial quantification: $0.05 = 5/100$

With additional data: $0.047 = 47/1000$

With Uncertainty Quantification



Rare-Event Data: Confidence Intervals

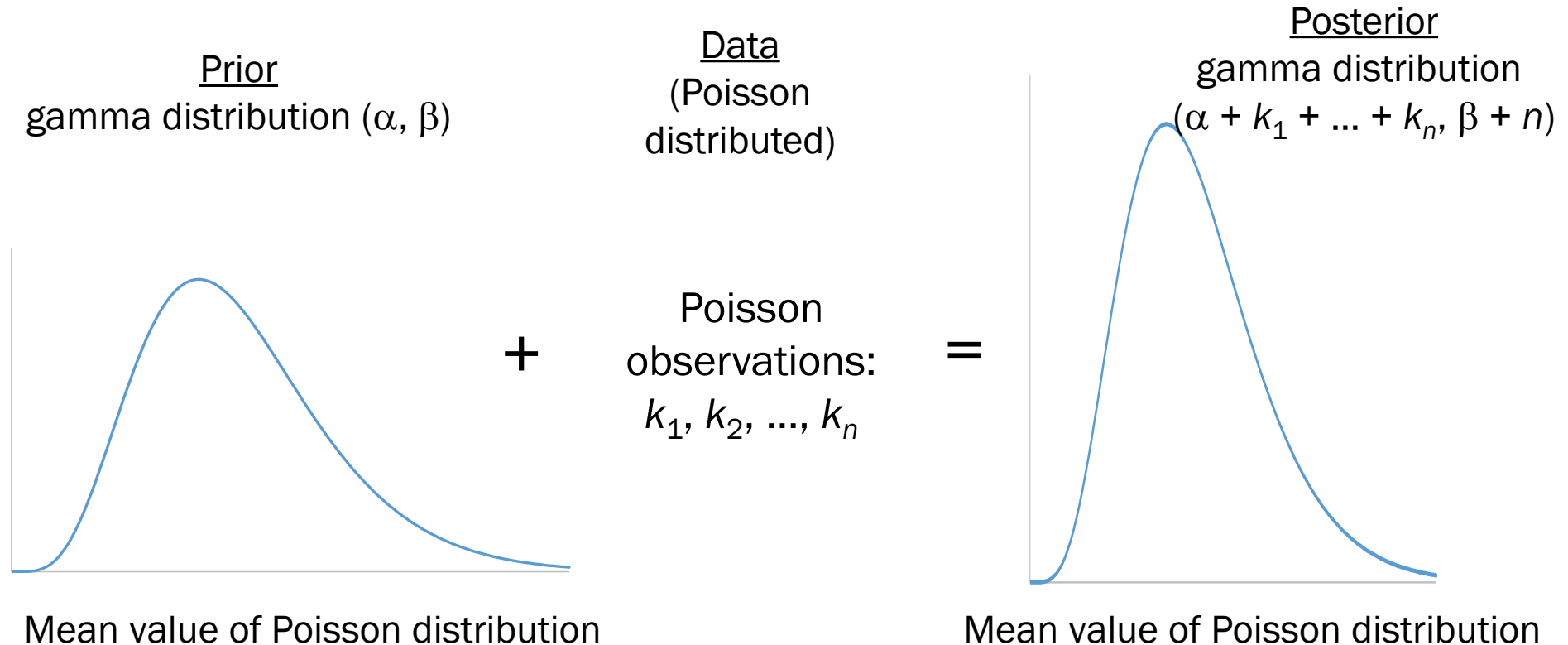
Confidence interval for mean of Poisson distribution:

$$[H_{2X}^{-1}(a/2)/2, H_{2X+2}^{-1}(1-a/2)/2]$$

- $H_k(x)$ = CDF of a χ^2 distribution with k degrees of freedom.
- X = observation of a Poisson random variable (a count of events)
- $1-\alpha$ = confidence level ($\alpha = 0.05 \rightarrow 95\%$ confidence interval)

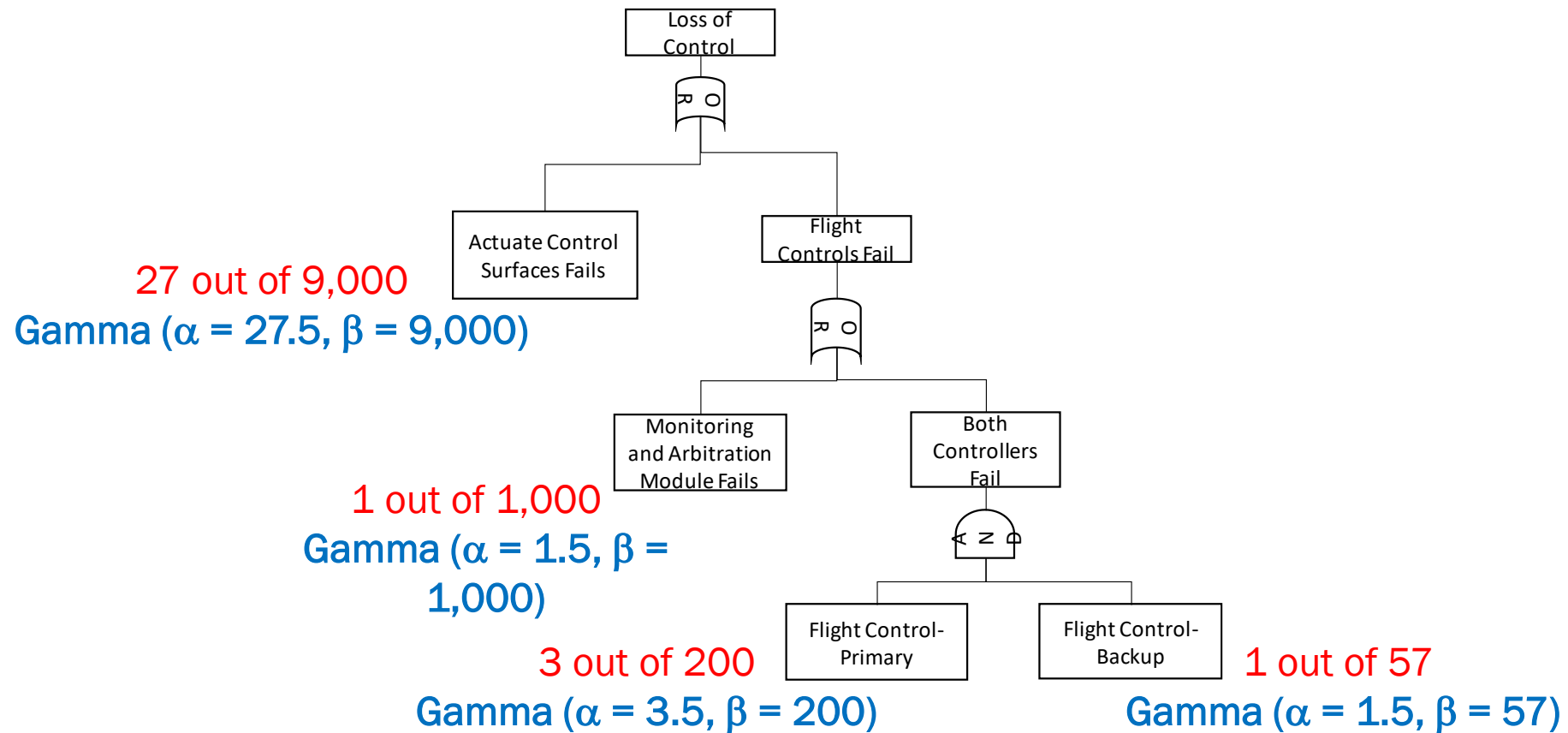
# Observations	Lower Bound	Upper Bound
0	0.00	3.69
1	0.03	5.57
2	0.24	7.22
3	0.62	8.77
4	1.09	10.24
5	1.62	11.67
6	2.20	13.06
7	2.81	14.42
8	3.45	15.76
9	4.12	17.08
10	4.80	18.39
15	8.40	24.74
20	12.22	30.89
25	16.18	36.90
30	20.24	42.83
35	24.38	48.68
40	28.58	54.47
45	32.82	60.21
50	37.11	65.92

Bayesian Updating for Poisson Data



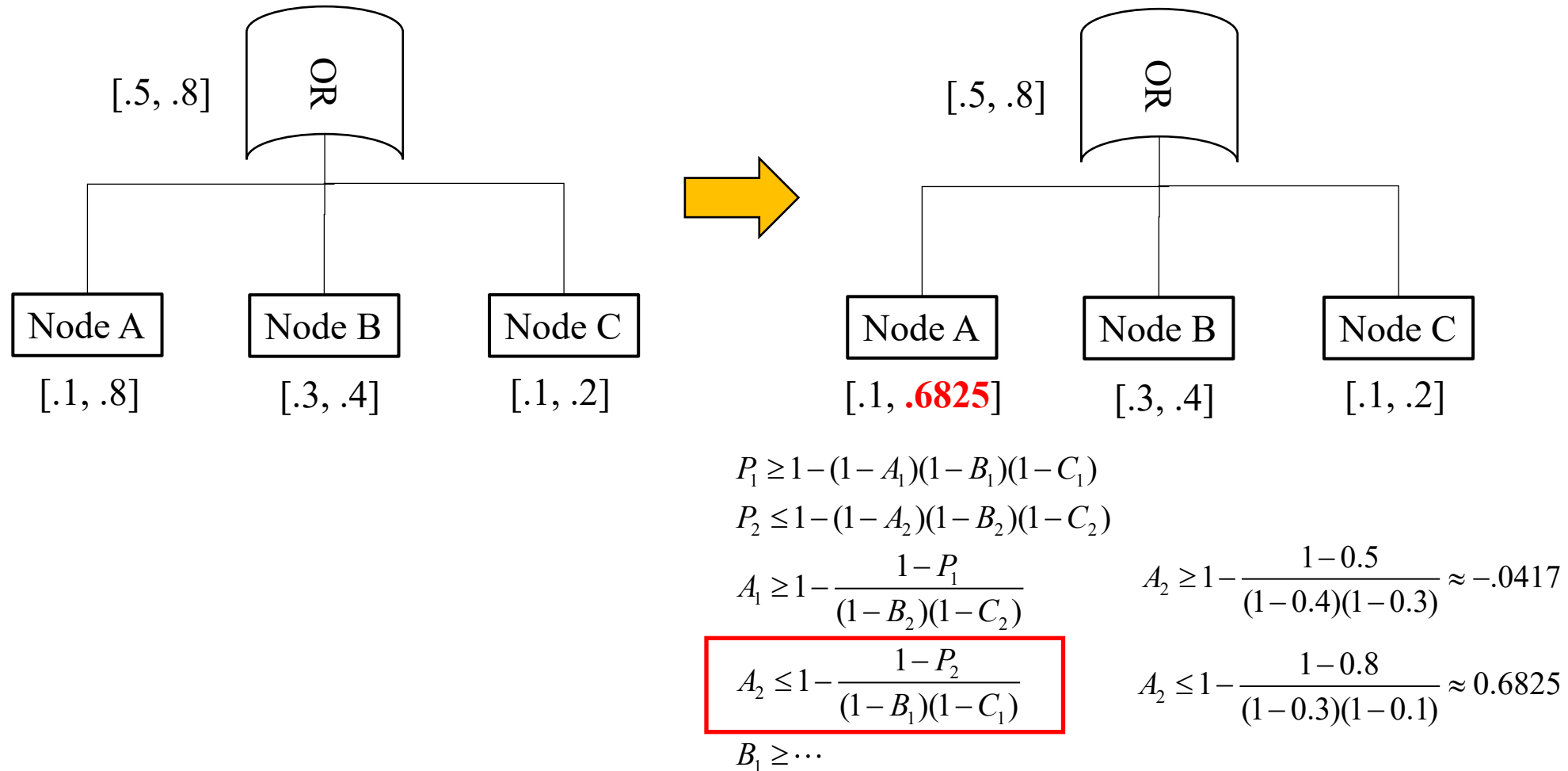
Bayesian approach provides 95% credible intervals $[a, b]$, similar to classical 95% confidence intervals, but also provides a full description of the uncertainty distribution

Example: All Nodes Quantified



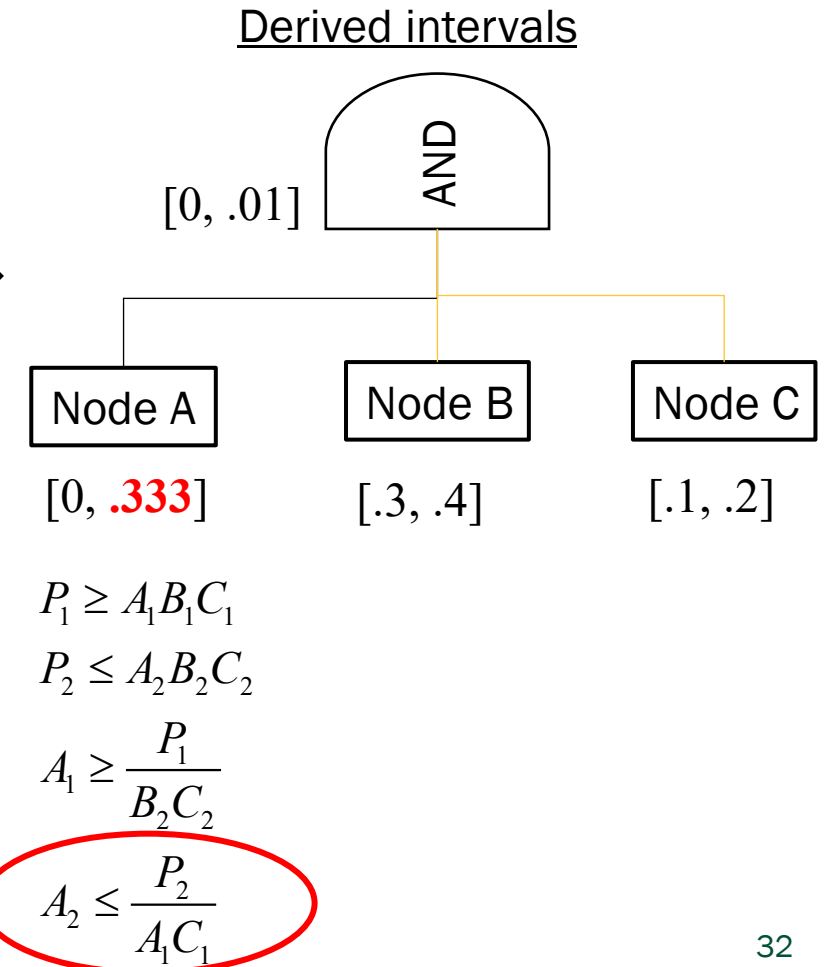
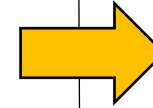
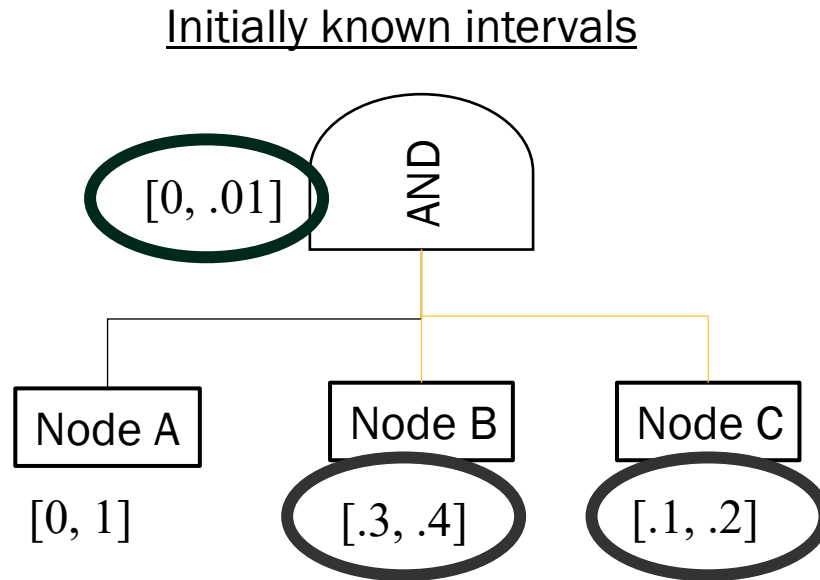
Test data used to quantified failure probability
Uncertainty distribution for failure probability

Interval Constraints, Example



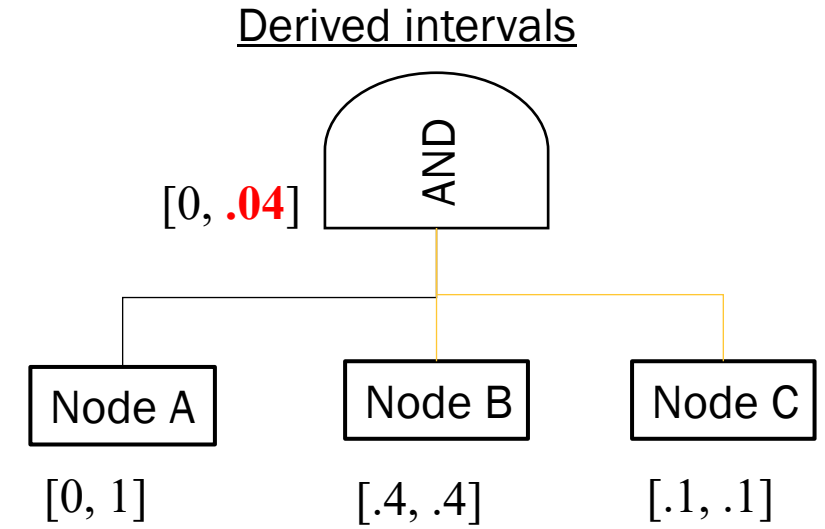
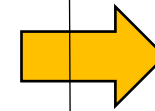
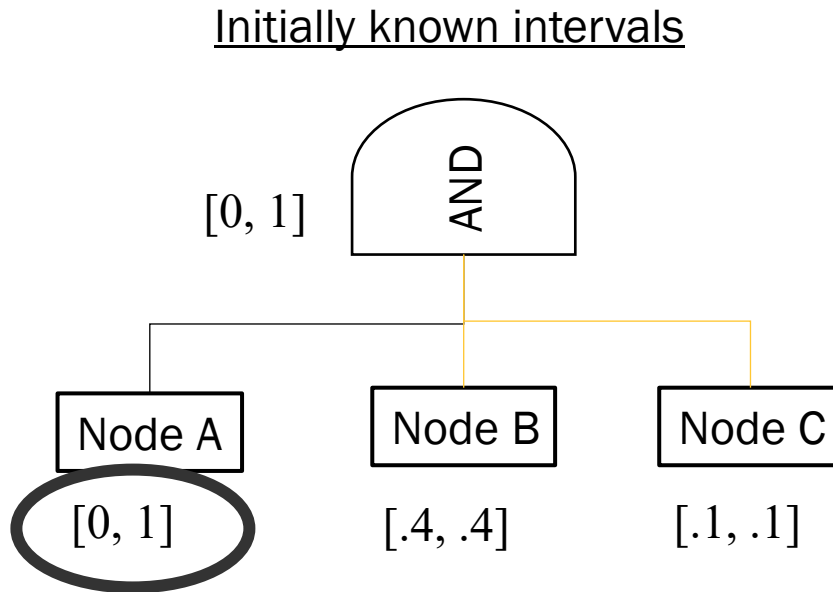
Interval Constraints, Example

- Top probability required $\leq .01$
- Nodes B and C quantified as intervals
- Requirements on A?



Interval Analysis

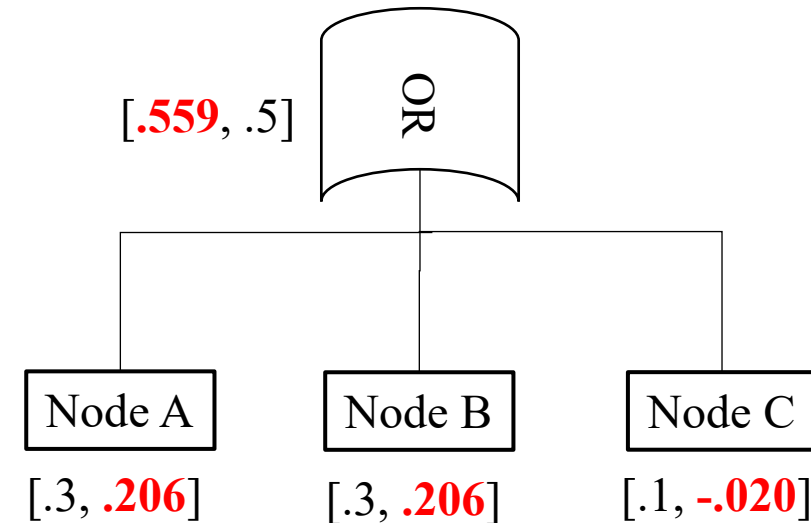
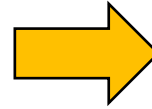
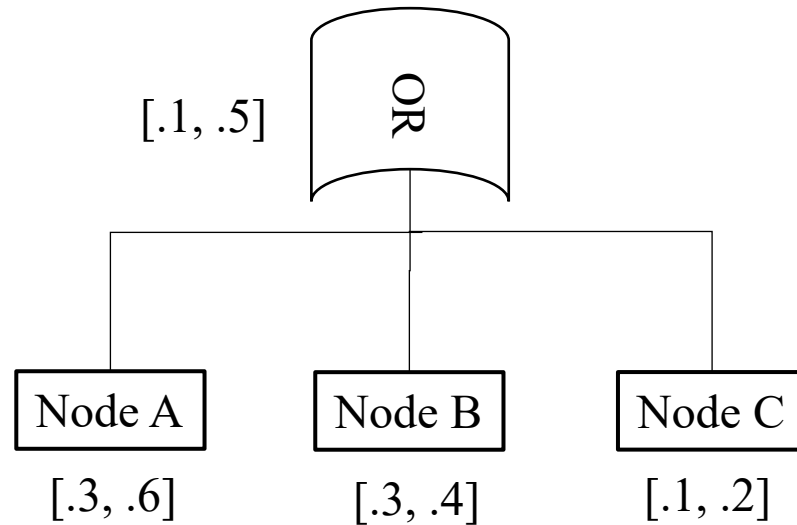
- Node A unknown (assign it [0,1])
- Nodes B and C known exactly



$P_1 \geq A_1 B_1 C_1$
 $P_2 \leq A_2 B_2 C_2$
 $A_1 \geq \frac{P_1}{B_2 C_2}$
 $A_2 \leq \frac{P_2}{A_1 C_1}$

- Calculate Interval for [P1, P2]

Example, Infeasible Tree



$$P_1 \geq 1 - (1 - A_1)(1 - B_1)(1 - C_1)$$

$$A_2 \leq 1 - \frac{1 - P_2}{(1 - B_1)(1 - C_1)}$$

$$B_2 \leq 1 - \frac{1 - P_2}{(1 - A_1)(1 - C_1)}$$

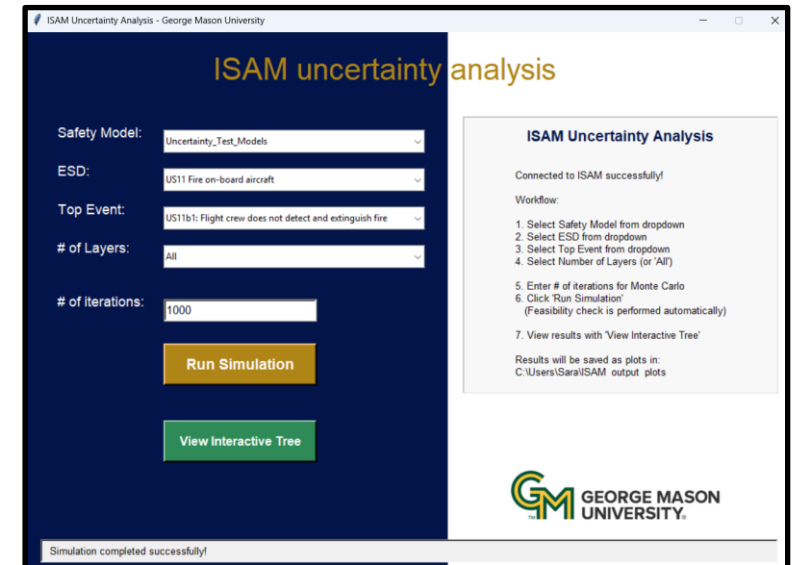
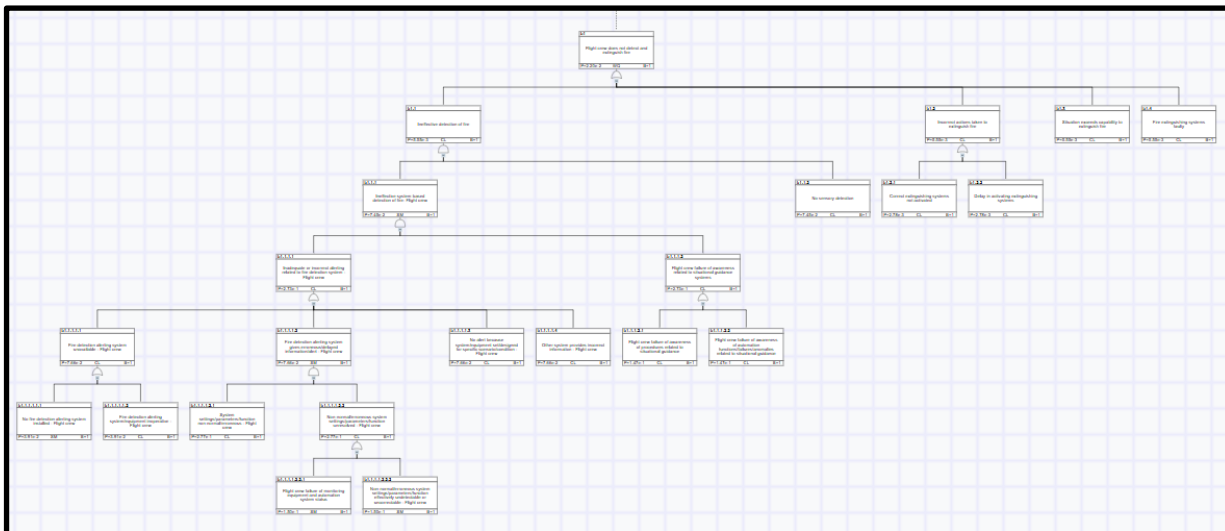
$$C_2 \leq 1 - \frac{1 - P_2}{(1 - A_1)(1 - B_1)}$$

If lower bound > upper bound for any node,
tree is infeasible based on initial quantification
(can occur from observed data if events are not
independent)

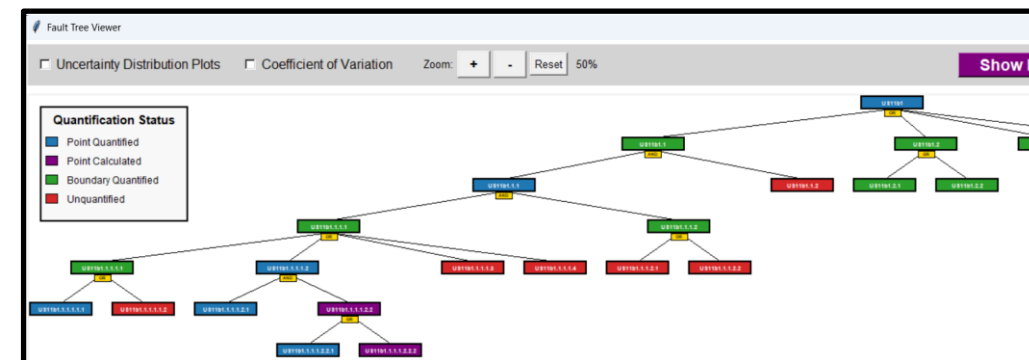
Uncertainty Quantification Tool

- Retrieves tree structure in a variety of formats
- Displays nodes with color-coded quantification status
- Computes uncertainty distributions, interval ranges, and uncertainty metrics for each node

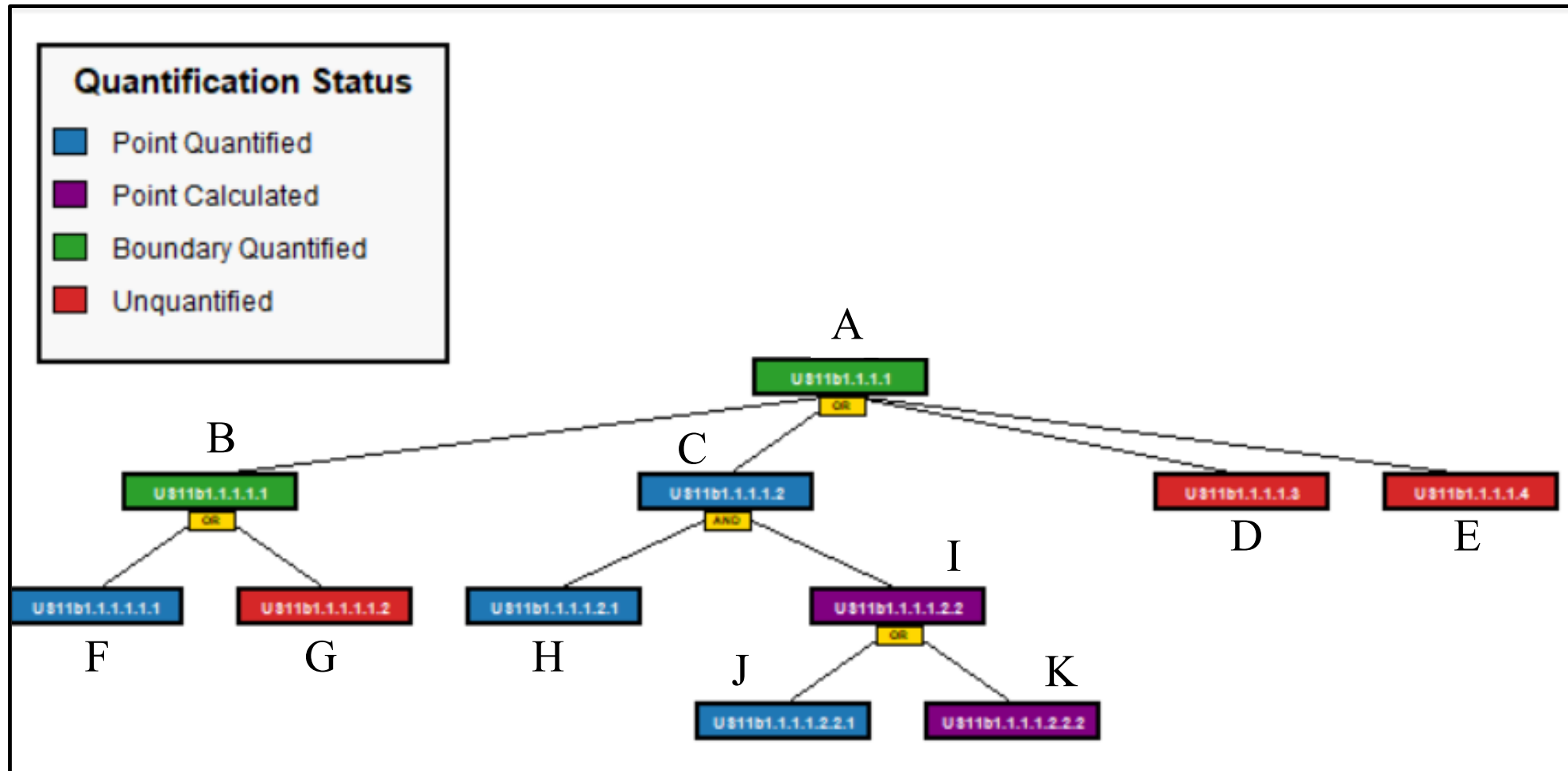
Fault Tree



Uncertainty Quantification

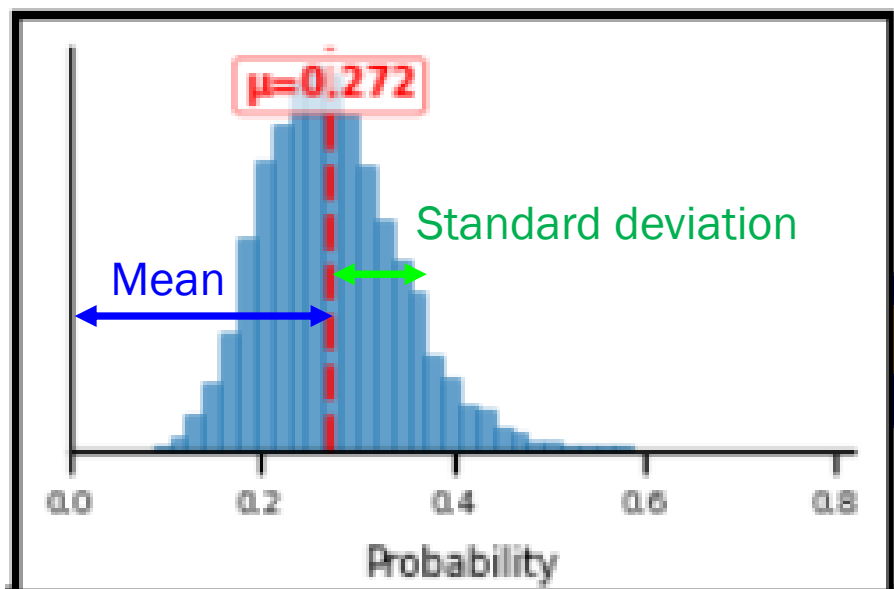


Quantification Status



Coef. of Variation

$$\text{Coefficient of variation} = \frac{\text{standard deviation}}{\text{mean}}$$



Measures level of uncertainty relative to the size of the estimated value, Useful single metric for “degree of uncertainty”

Quantification Categories

- Point Quantified
- Point Calculated
- Boundary Quantified
- Unquantified

CV Categories

- Very Low (<0.1)
- Low (0.1-0.25)
- Medium (0.25-0.4)
- High (0.4-0.577)
- Uniform or Higher (≥ 0.577)

Coefficient of Variation Analysis

