Markov Modeling Application to a Redundant Safety System

George Adams and Fernando Ferrante
Center for Nuclear Waste Regulatory Analyses

ASME Power 2007 Conference
San Antonio, Texas

July 17, 2007

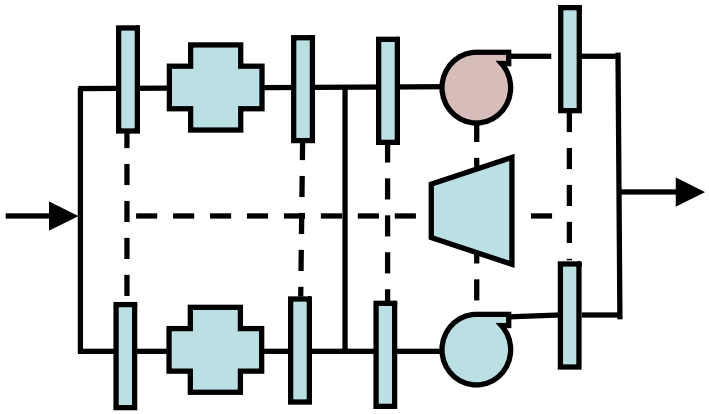
CNWRA
A center of excellence in earth sciences and engineering™

Outline

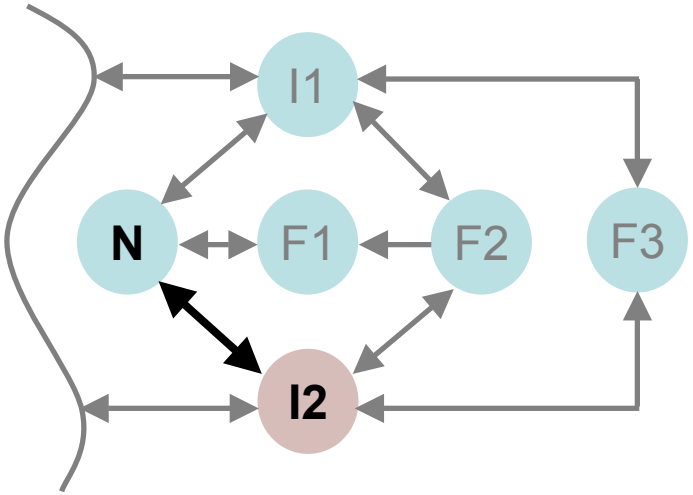
- Background and objectives
- Hypothetical HVAC exhaust system description
- Fault tree modeling
- Markov modeling
- Results from Markov and fault tree models
- Conclusions

Background

- For reliable, complex engineering systems
  - Redundancy is part of the design
  - May have one or more operating states
  - May have one or more failed states



Hypothetical HVAC Exhaust System



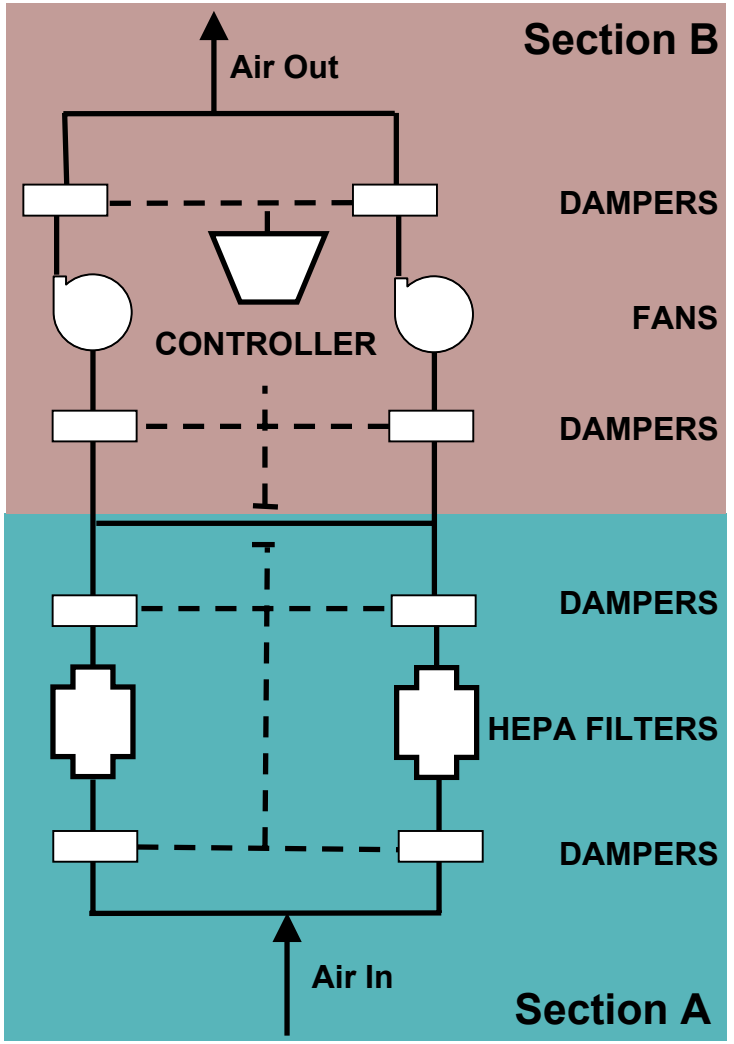
Markov Model showing Discrete System States

Objective

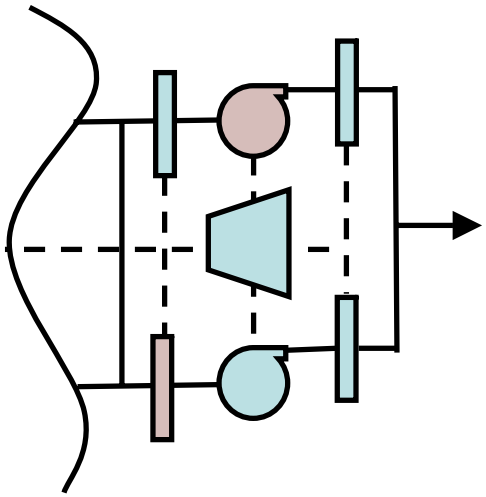
- Use Markov model to better capture
  - Redundancy of components
  - Maintenance intervals
  - Repair and restoration of components
- Compare Markov modeling to fault tree modeling

Hypothetical HVAC Exhaust System

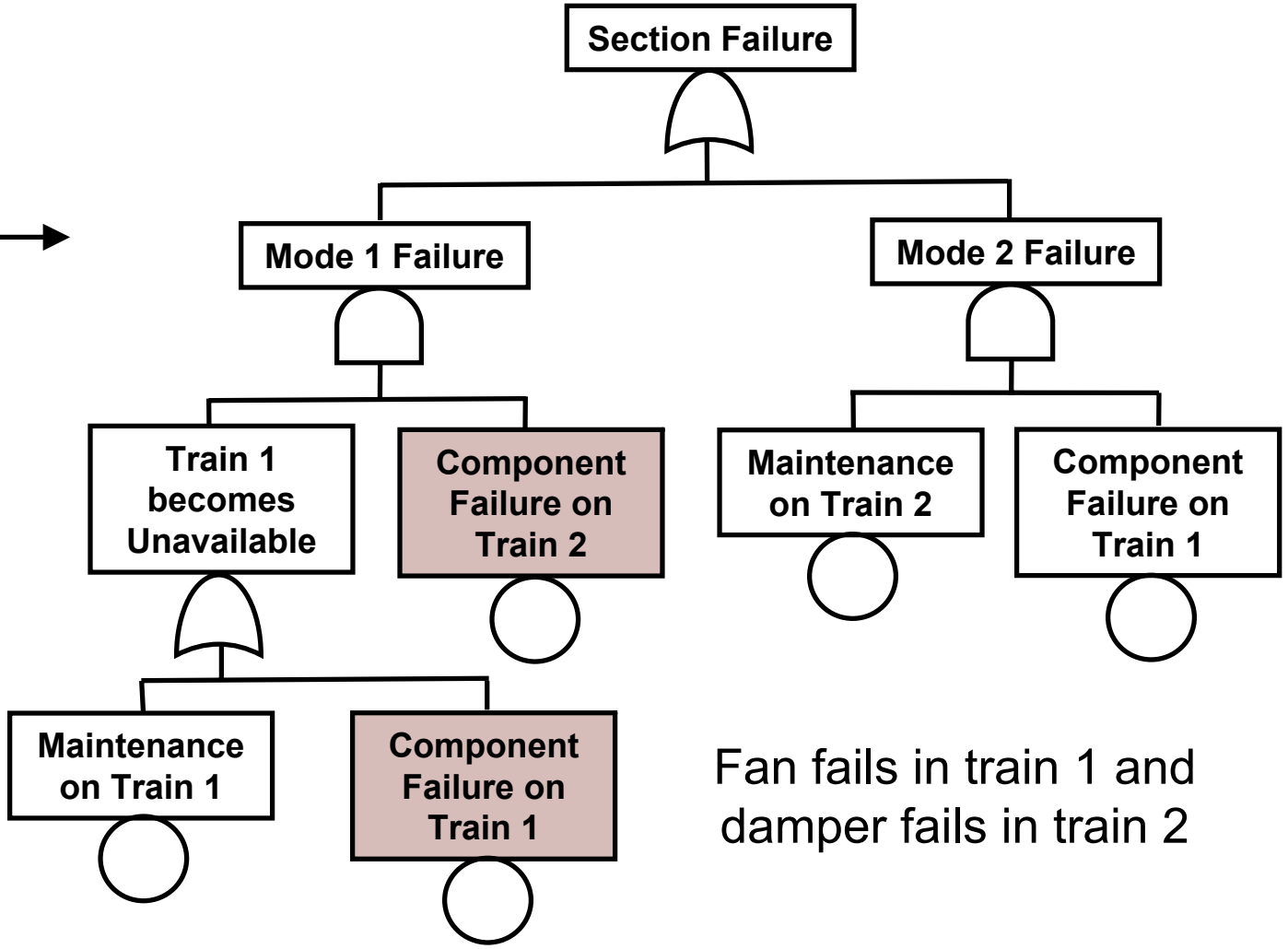
- Continuously operating safety system
- Intermediate state
  - Component fails and is undergoing repair
  - Maintenance is being performed
- Failed state
  - More than one component fails
  - Failure occurs during maintenance
- System performance described through discrete states



Fault Tree Model

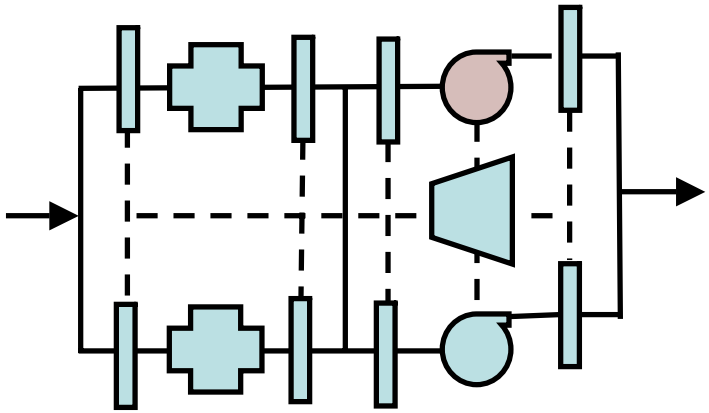


Failed State

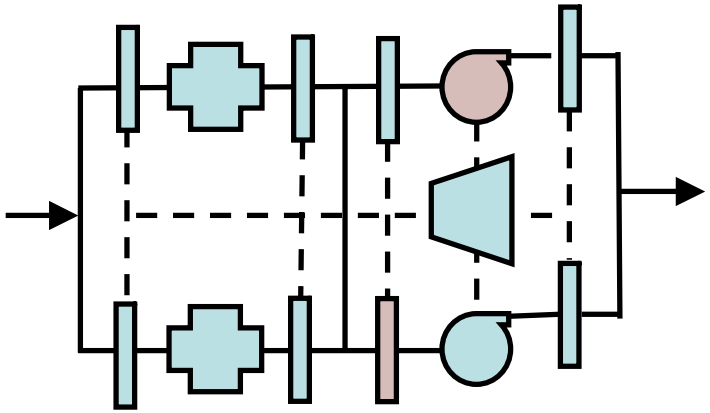


Fan fails in train 1 and damper fails in train 2

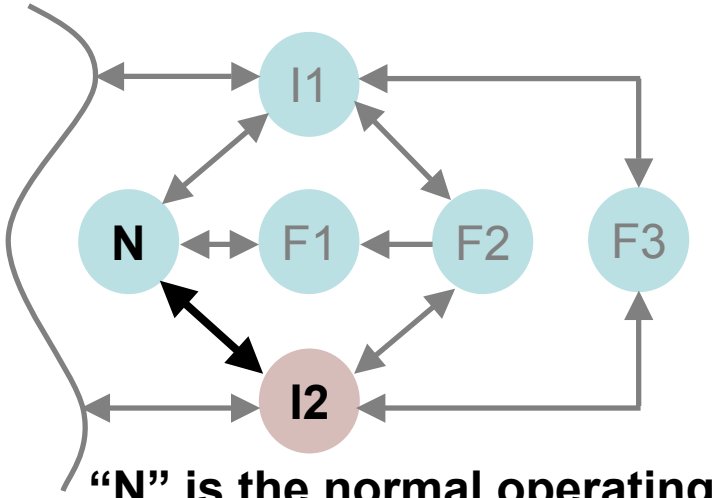
Markov Model—HVAC System



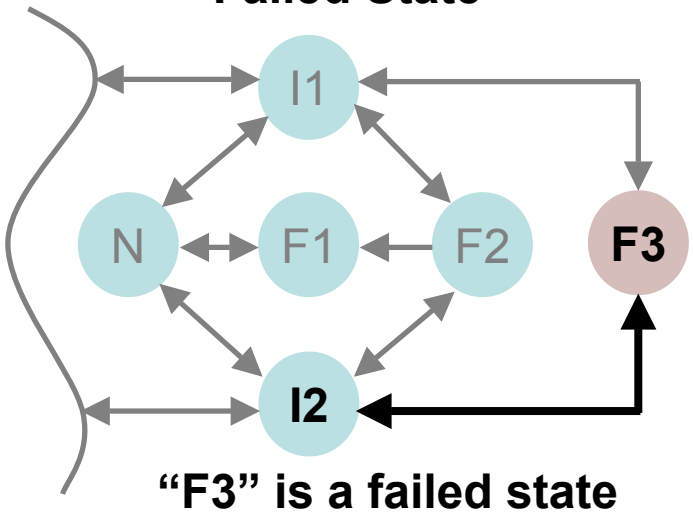
Intermediate State



Failed State

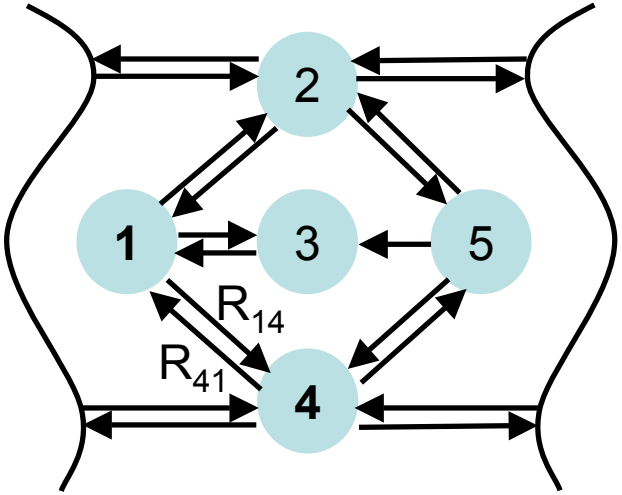


“N” is the normal operating state
“I2” is an intermediate state



“F3” is a failed state

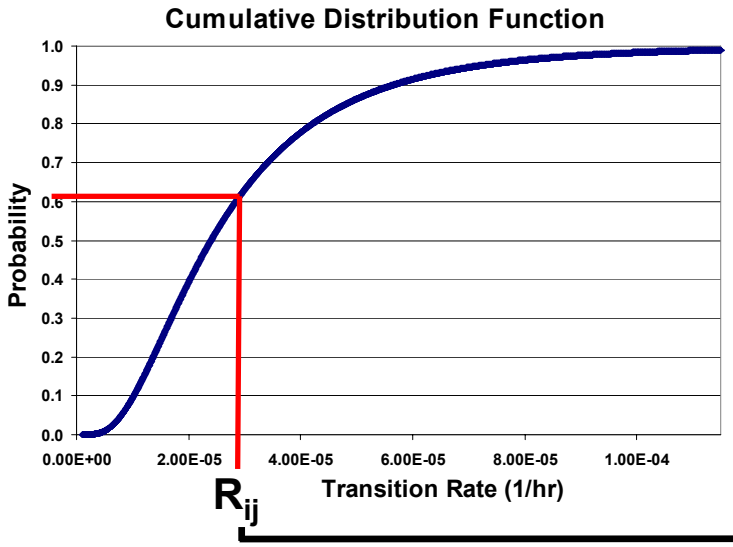
Analytical Markov



$$\begin{array}{c} \\ 1 \\ 2 \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & \cdots & i \end{array} \\ \begin{bmatrix} R_{11} & R_{12} & \cdots & R_{1j} \\ R_{21} & R_{22} & \cdots & R_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ & & & R_{ij} \end{bmatrix} \end{array}$$

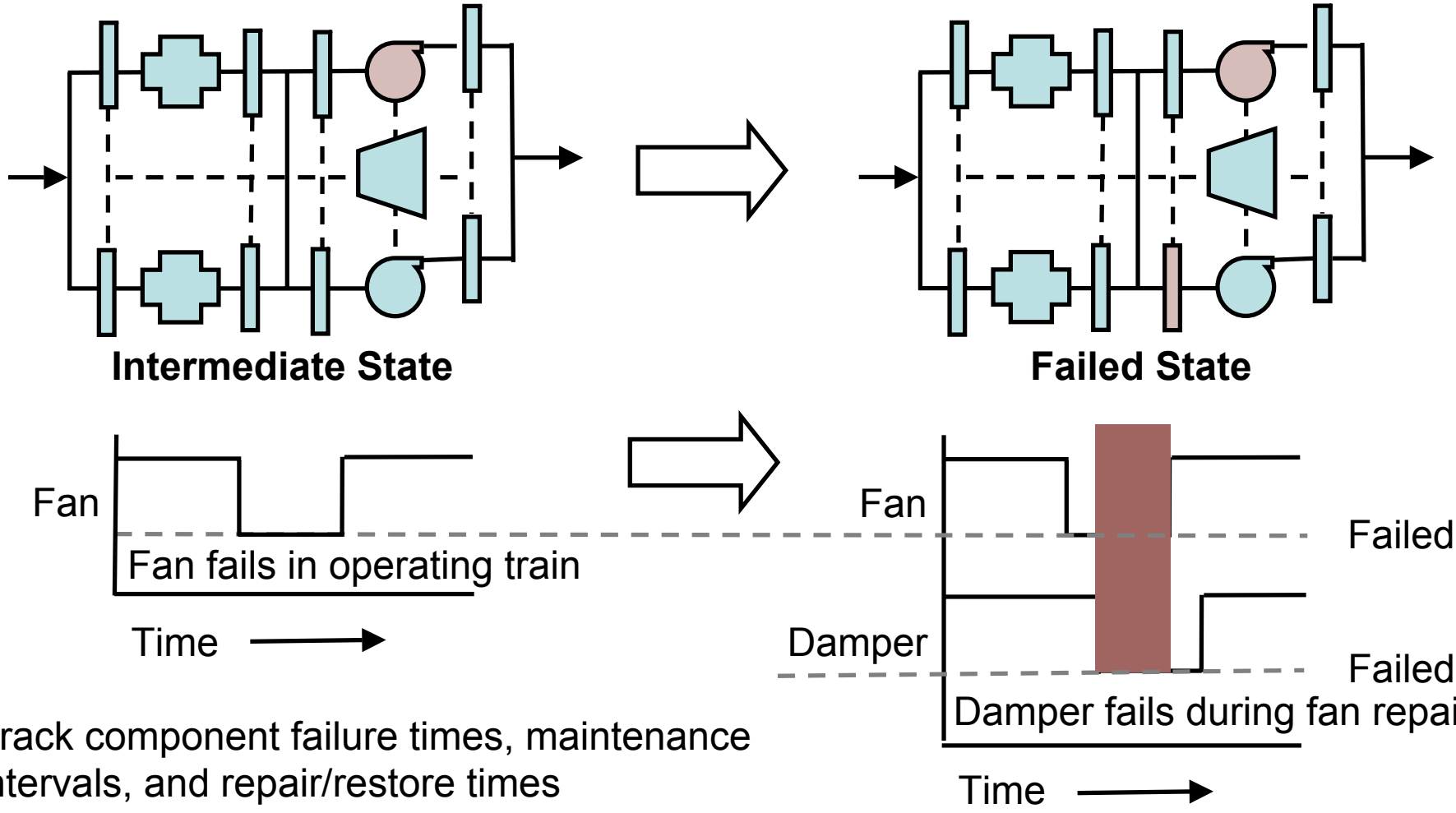
Stochastic transition probability matrix truncated (i.e., rows and columns removed) for the failed states

Uncertainty Analysis



Sampled values may be input directly into the truncated stochastic transition probability matrix

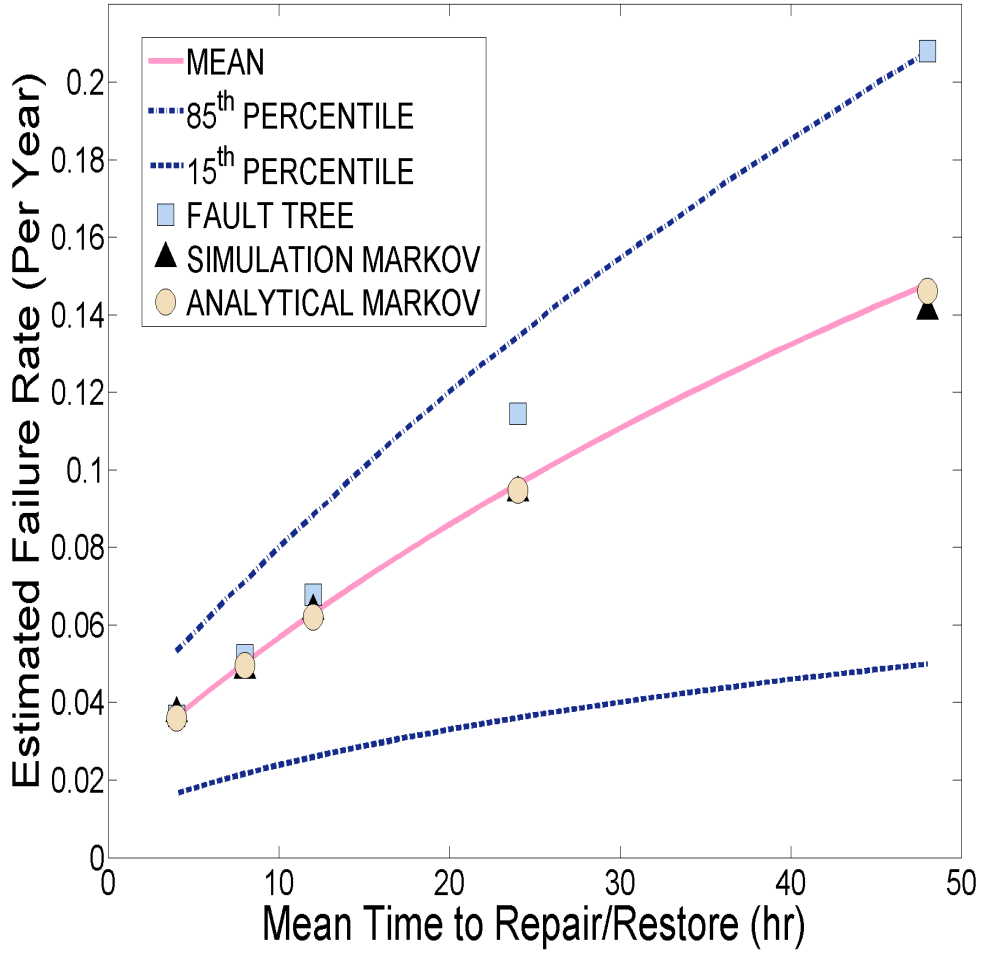
Simulation Markov



Track component failure times, maintenance intervals, and repair/restore times

Model Comparison

- Analytical Markov and simulation Markov failure rates compare well
- Fault tree and Markov estimates diverge as the mean times to repair a component or restore from maintenance increase



Conclusion

- Intermediate states may play a significant role in estimating the system failure rate
- Markov techniques may generate a more realistic (i.e., less conservative) estimate than fault tree
- Can be extended to more complex systems

Acknowledgements

This presentation was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the U.S. Nuclear Regulatory Commission (NRC) under Contract No. NRC-02-02-012. The activities reported here were performed on behalf of the NRC Office of Nuclear Material Safety and Safeguards, Division of High-Level Waste Repository Safety.

This paper is an independent product of CNWRA and does not necessarily reflect the views or regulatory position of NRC.