

Reliability Physics Based On Causal Dynamic Networks

- **RAPSODE** -

Simone B. Bortolami, PhD

IEEE Reliability – Boston Chapter
Massachusetts Institute of Technology Lincoln Laboratory
March 09, 2016

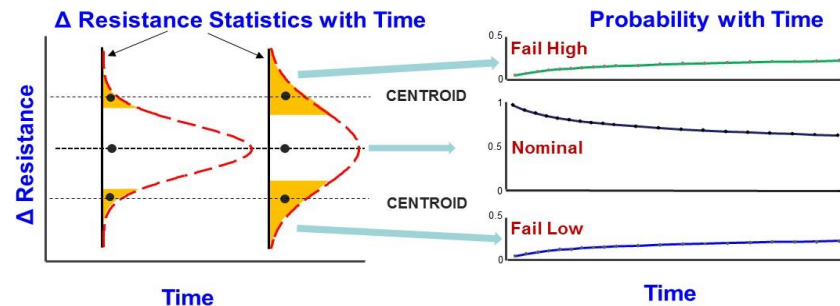
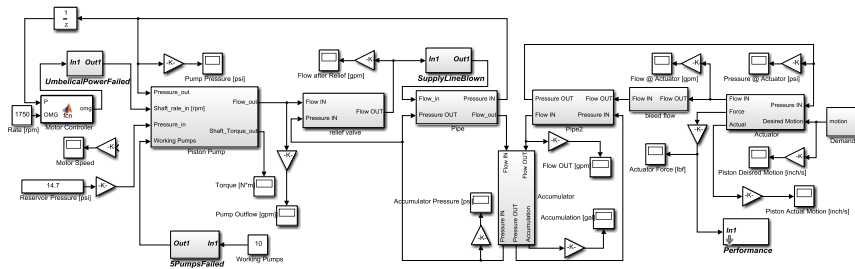
Draper publication P-6735

Abstract

Complex one-of-a-kind systems are usually built to stringent performance and/or reliability requirements. Nevertheless, they remain vulnerable to catastrophic events that are often a combination of individually nonfatal events and/or processes. Also, the reliability of such systems does not commonly involve catastrophe, but rather an unexpected degradation of performance affecting the cost of maintenance and/or ownership. Thus, lack of reliability does not necessarily mean loss of the use of a system, but also a decay of performance below a set threshold. Physics of failure (PoF) has been the practice in several fields of engineering primarily involved with their design for life expectancy, e.g., fatigue, corrosion, etc. New simulation-based approaches have been used to address mission reliability by evaluating the impact of single failures to the key outputs of the system during its operation. RAPSODE is a proposed approach that uses behavioral models of the system's dynamics and embedded PoF models to evaluate the outcome of all combinations of failure and/or degradation sources, which are different for different environments and mission goals. RAPSODE uses causal networks to identify all possible failure/degradation states. At the design stage, RAPSODE helps isolate, among all critical paths, the ones with the highest influence on mission reliability, thereby driving targeted laboratory tests and fault-tolerant design. RAPSODE can be also used to analyze complex systems with a human-in-the-loop.

Contents and Significance

- **RAPSODE** is a method that combines behavioral models of complex systems with Physics of Failure (PoF) models to capture hard failures, degraded performance of components/subsystems, and other risks, in a seamless manner
 - Behavioral models are state-based Markov or non-Markov processes
 - PoF models combine physics with statistics



Contents and Significance (cont'd)

RAPSODE:

- Identifies and characterizes risk for failure modes that are too complex to be identified solely through intuition
- Identifies causes for degraded system performance and characterizes their risk
- Identifies and characterizes risks deriving from changes in environmental conditions
- Identifies and characterizes complex phenomena deriving from component interactions during field operation
- Extends reliability metric based on component failure with system performance and cost of ownership metrics

Complex High-Reliability One-of-a-Kind Systems

Examples



Source: World Wide Web

Common Characteristics

- Engineered to avoid catastrophic failures
- Designed and built to have very long lives
- Limited quantities from one to a few hundreds
- Continuous operation or/and extreme environments
- Deployed in remote or inaccessible locations
- Downtime might be unacceptable or catastrophic
- Because the high cost of development and even higher cost of sustainment, they need to minimize the cost of ownership to be practical
- Scarce failure data and/or available only from dissimilar systems

Type of Failures Not Well Treated by Traditional Methods

- Cascading failures
 - e.g., Power failure → removes cooling → effects avionics ...
- Catastrophic event involving 3rd or higher failure level
 - e.g., String A power + String B computer + String C cooling
- Slow degradation of components and/or unforeseen phenomena and/or interactions developing during field operation result in:
 - Unexplainable degradation of system performance
 - Higher than expected repair effort and costs
 - Lower than expected availability
 - Higher than expected down time
 - Reduced life expectancy
- Human-in-the-loop error
 - e.g., unexpected software output to unforeseen input → incorrect hardware/software override by human misunderstanding



NOTE: RAPSODE can be extended to address software reliability, but the subject is not treated in here

Existing Foundations of Reliability Methods

- Mean Time Between Failure (MTBF) data from catalogs used in:
 - Part stress/part count analyses and similar
 - Failure mode and effects analysis (FMEA, FMECA) and similar
- PoF analyses also used in:
 - Mechanical and thermal fatigue design analyses
 - FEM and CFD for static and dynamic load analyses
 - Electrical design, corrosion, diffusion, and similar analyses
- Monte Carlo simulations
- Dependency-type analyses, fault trees, Markov chains, and similar
- Reliability Block Diagrams (RBD), Bayesian Decomposition, and others

Limitations of Traditional Methods

- FMEA and dependency type approaches cannot easily deal with failure interactions beyond the first level
- RBDs and Fault Trees have difficulty dealing with partially cross-strapped architectures
- Methods based on analysis of components do not usually account for complex interactions phenomena
- Analyses based on constant failure rates (MTBF) can handle large systems, but might yield inaccurate results
- Methods based on PoF address time and mission-dependent loads, but are not yet system approaches
- Established reliability methods were not originally constructed to analyze human-in-the-loop
- Markov modeling and similar methods are powerful, but not yet widely adopted

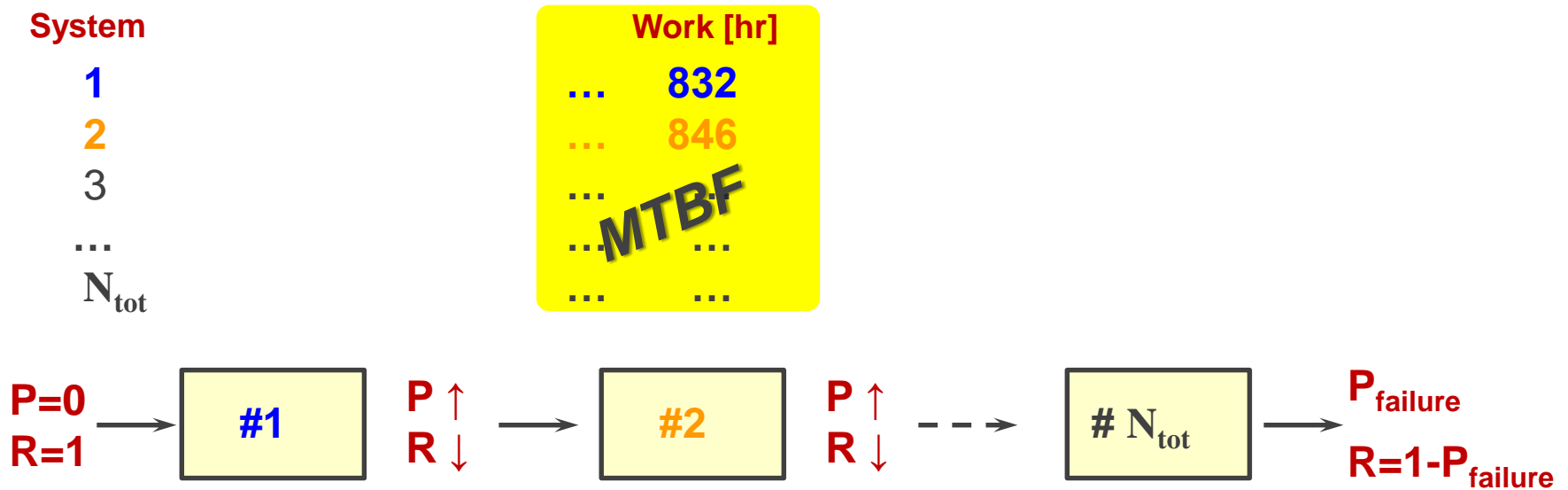
RAPSODE's Key Features

- Model based **[Bracketed numbers are references listed on page 36]**
 - Whole system approach extending single component failure
 - Leverages on knowledge/models already generated by system design and analysis efforts
 - Traditional component MTBFs are used in conjunction with PoF
- Autonomously generates all failure paths and trees
 - Including cascading failures and failures beyond 3rd level
 - Adopts discipline's best practices, e.g., **[1, 2]**
 - Allows for fault-tolerant design via sensitivity analysis **[cf. 5]**
- Associates degradation functions, “soft-failures,” to nonfatal phenomena (PoFs) affecting a system, e.g.
 - Degradation of material properties, biases, drifts, gain shifts...

RAPSODE's Key Features (cont'd)

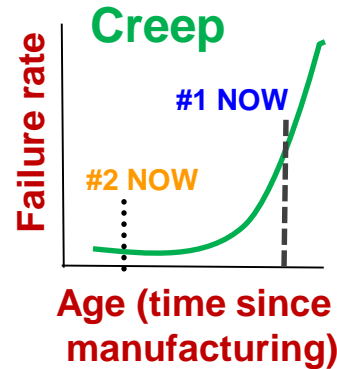
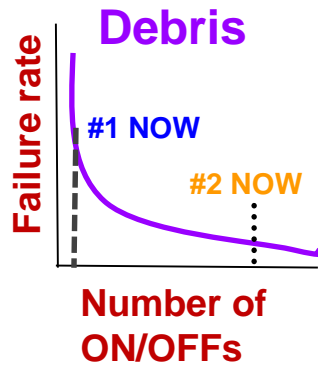
- Interdependency and interactions among subsystems
- Changes in the environment
- Human actions/interactions, different as circumstances change
- (Soft failures, in particular association, conditions, that with time might lead to bad performance and/or system failure)
- Identifies true drivers for PoF mechanisms and models
- Yields live reliability models of systems or families of products in the field
- Adds new metrics to traditional mission reliability
 - Cost of ownership
 - System performance

EXAMPLE: Reliability of a Whole Product Family



Reliability of a Whole Product Family (cont'd)

PoF 1
&
PoF 2

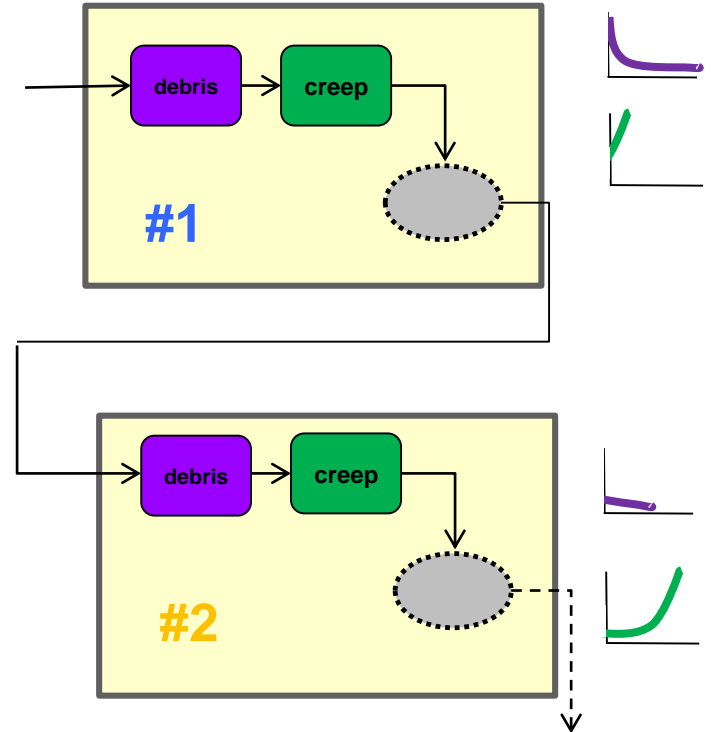
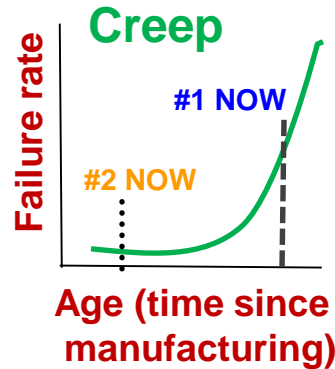
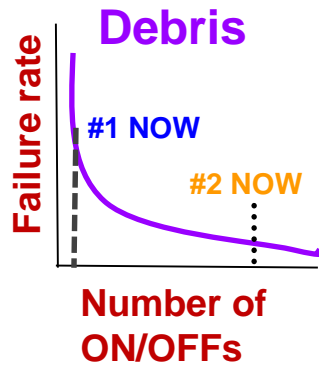


System	ON/OFFs	Age [yr]
1	7	7.44
2	49	1.12
3
...
N_{tot}

RAPSODE

Reliability of a Whole Product Family (cont'd)

PoF 1
&
PoF 2



System	ON/OFFs	Age [yr]
1	7	7.44
2	49	1.12
3
...
N_{tot}

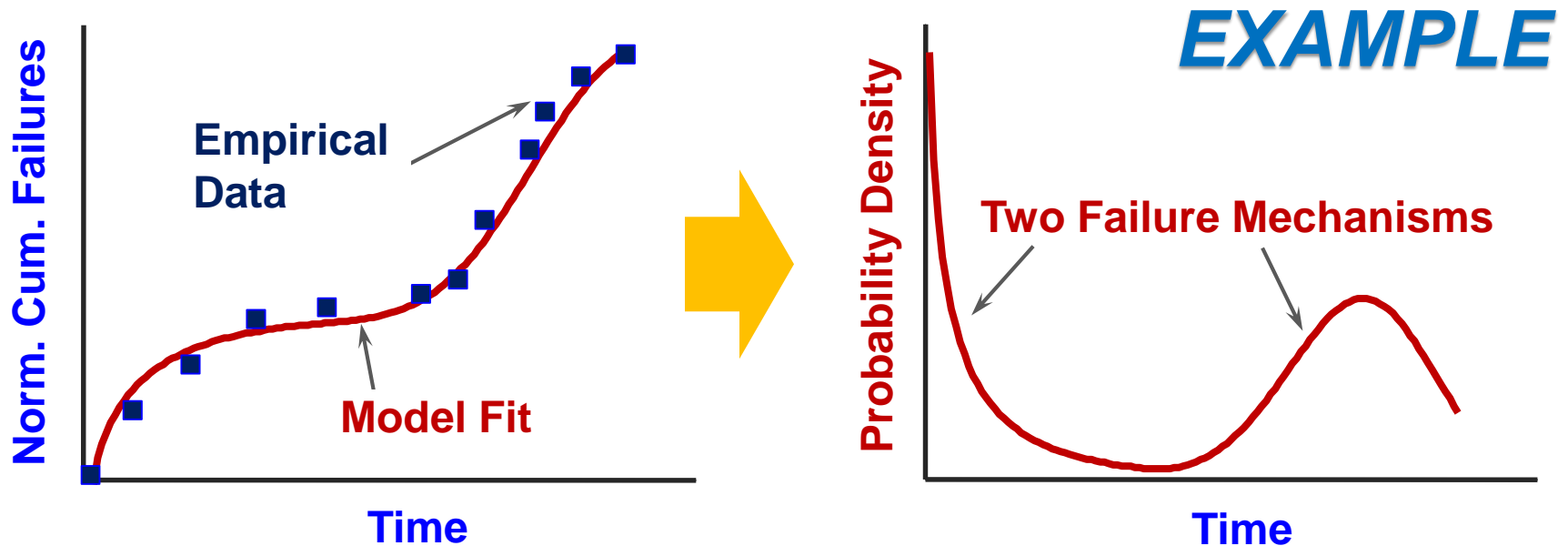
RAPSODE



Empirical and Analytical PoF

- The system's model can embed *traditional failure types* for components with MBTFs from catalogs
- In addition, *Empirical PoF* models (**E-PoF**) can also be added to capture phenomena mainly affecting the functioning of the system, which might be:
 - Changes in material properties, particle cluttering, wear out, aging, creep, corrosion, environment, etc.
 - E-PoF are identified and modeled from pertinent field or laboratory data or from dissimilar systems that have been affected by the same phenomena
- *Analytical PoFs* (**A-PoF**) are similar, but derived from analyses, e.g., FEM and/or dedicated laboratory tests of material/component properties

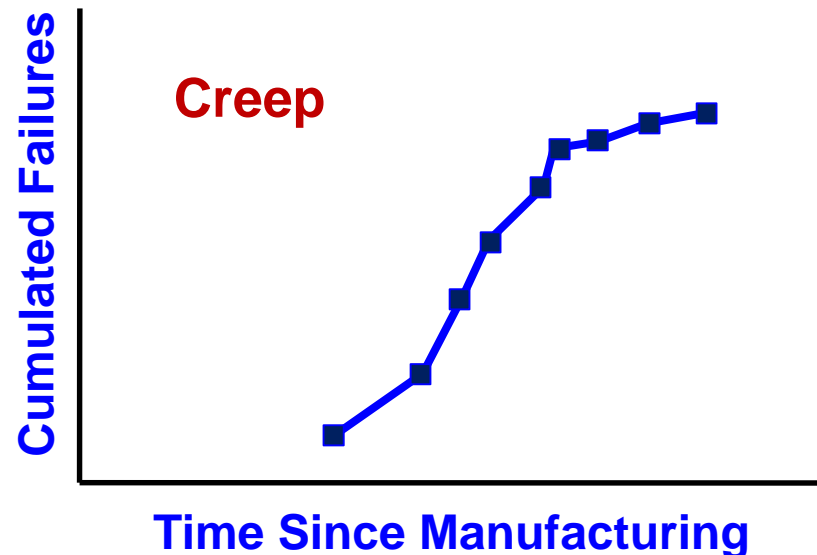
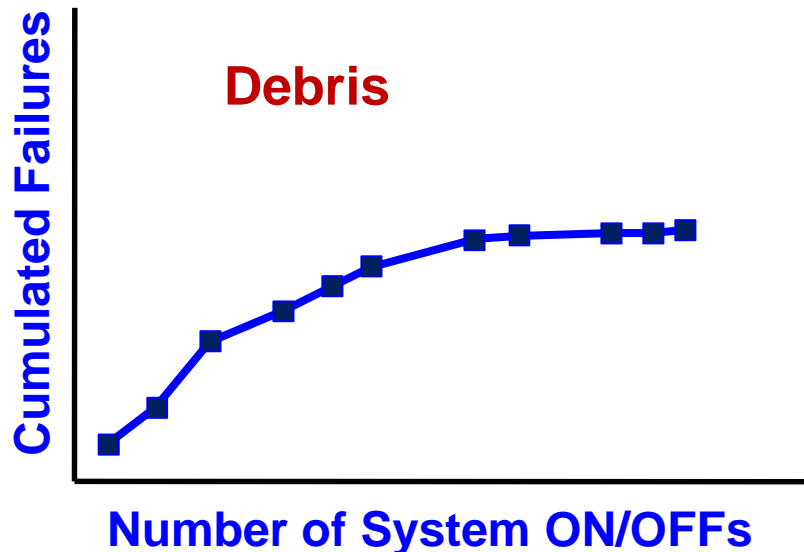
Data Mining for Empirical PoF Models (E-PoF)



- Available data might be from different systems, but operating in similar environments
 - Forensic data are usually discontinuous and inconclusive
- Identify underlying statistics and cross-reference with forensic root-cause reports to yield insights

Data Mining for Empirical PoF Models (E-PoF) (cont'd)

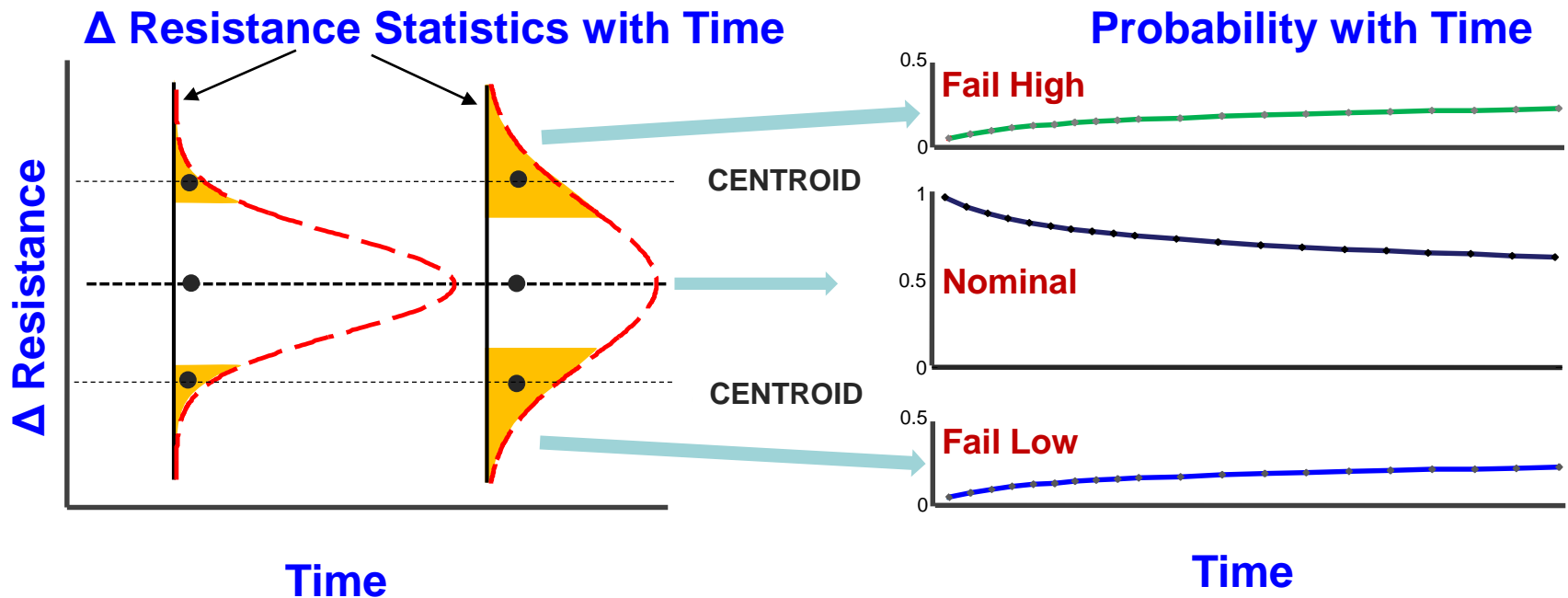
- Insights help identify driving variables of PoFs, e.g.,
 - Debris in fluids is stirred up by ON/OFFs and, if present, shows up early on yielding an infant-mortality type of failure
 - Change in physical properties, aging, creep, develops with time even during dormancy and is a wear-out type of failure
- Fitting statistical models with correct variables helps explain raw data and yield PoF hazard functions



Deriving Analytical PoF Models (A-PoF)

- Matching precision resistors (identical resistance) in precision voltage divider that is part of a larger system
 - Resistors are hand picked from same production batch
 - Resistors have same aging statistics

EXAMPLE



Deriving Analytical PoF Models (A-PoF) (cont'd)

- Failure occurs when resistors drift apart
- Matching aging statistics yields zero expected value for relative drift
- However, probability of zero relative drift changes with time
- Two PoF mechanisms are derived
 - First is the difference in resistor resistances being above a set value (fail high)
 - Second is the same being below a set value (fail low)
- Derived probabilities with time yield PoF hazard functions

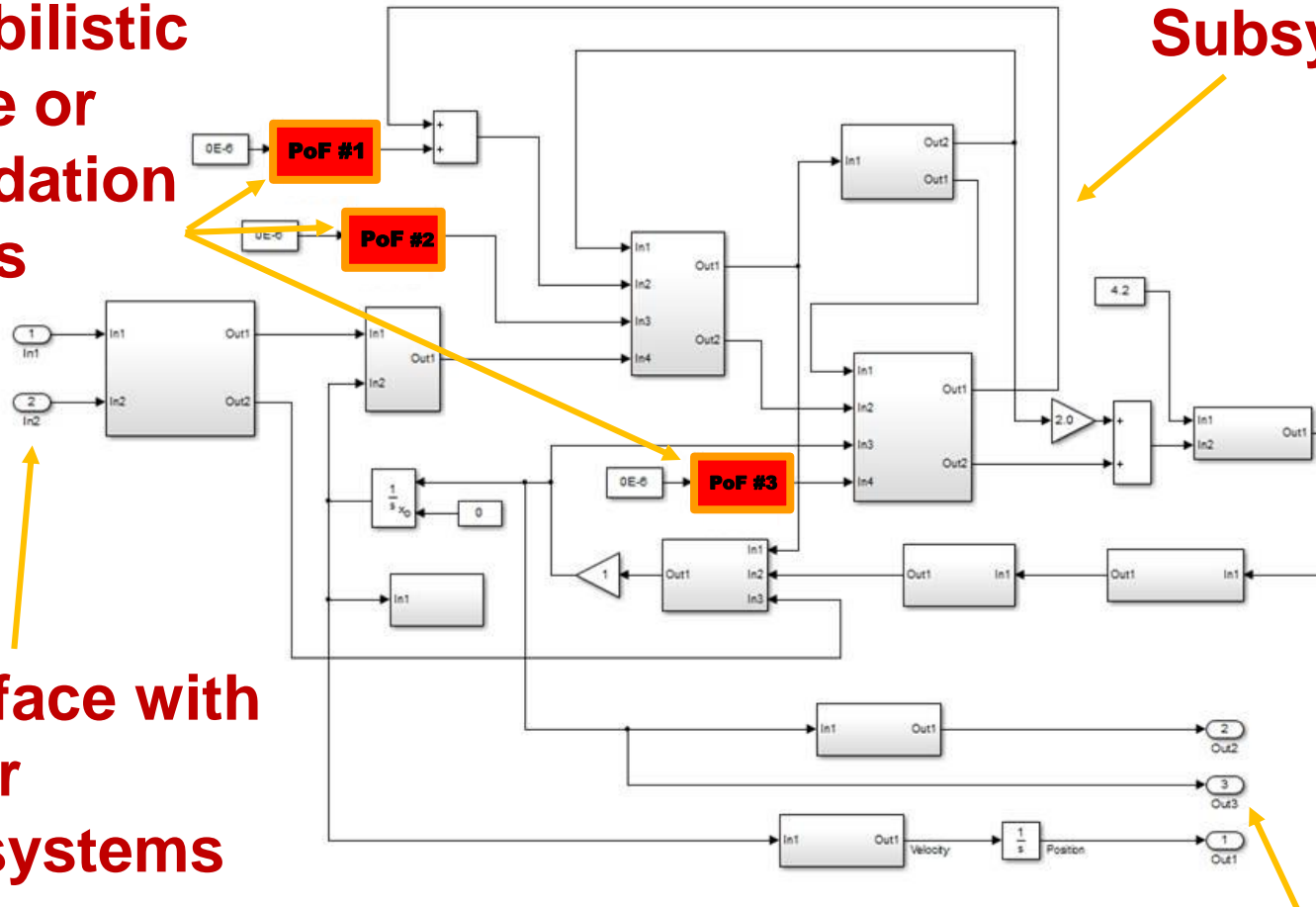
RAPSODE Uses Behavioral Models of Mission

- Behavioral models capture system functions starting from inputs and outputs
- They do not need to be high-fidelity dynamics models
- Behavioral models only deal with measurable input/outputs available from the field (called observables)
- Behavioral models are built to be computationally light and fast
- RAPSODE guides model development by progressively identifying the subsystems that most impact the overall mission's reliability, e.g., cf. **[5]**
- Model-based methods like RAPSODE allow for fast design iterations as plant and mission evolve

New and Old Failures Types Are Added to Model

Probabilistic Failure or Degradation Models

Subsystem

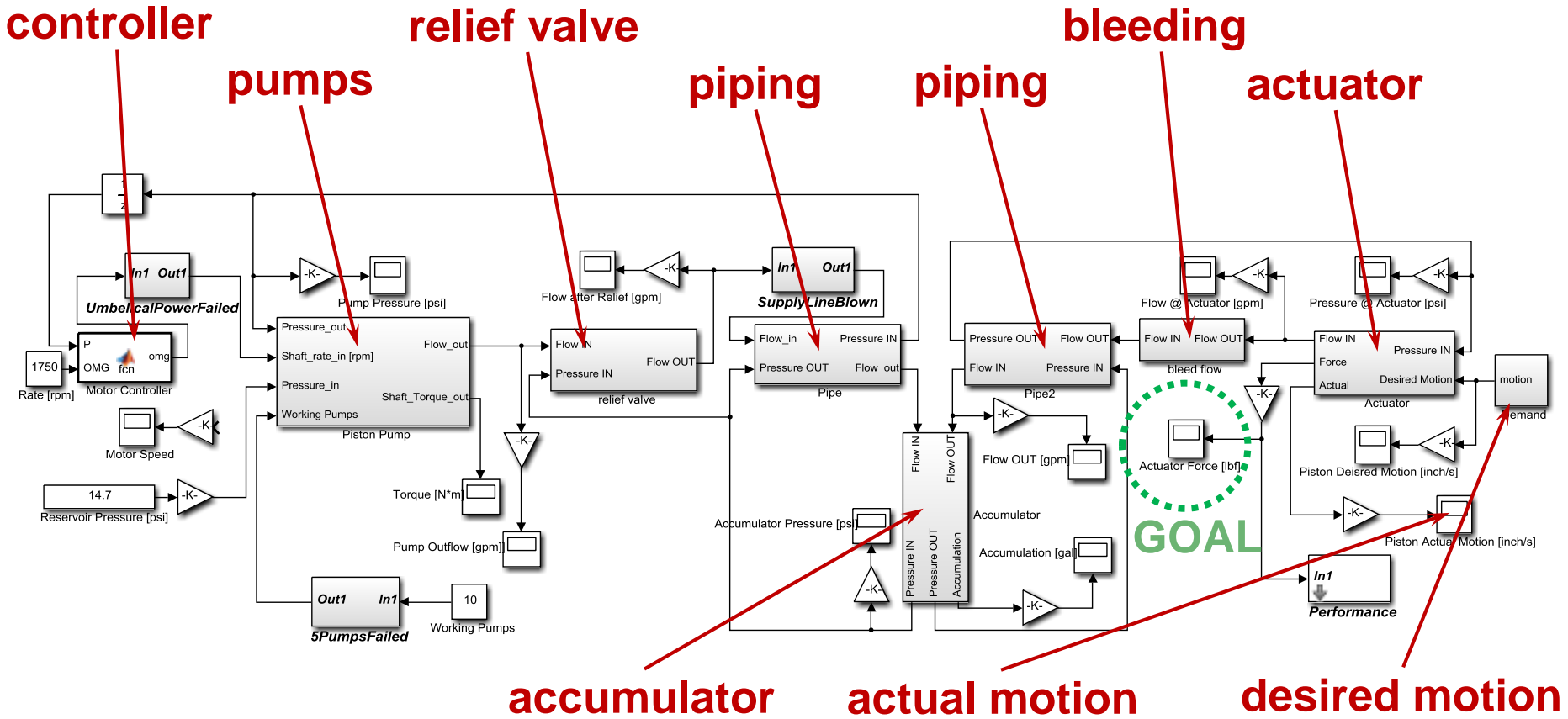


Interface with Other Subsystems

Interface with Other Subsystems

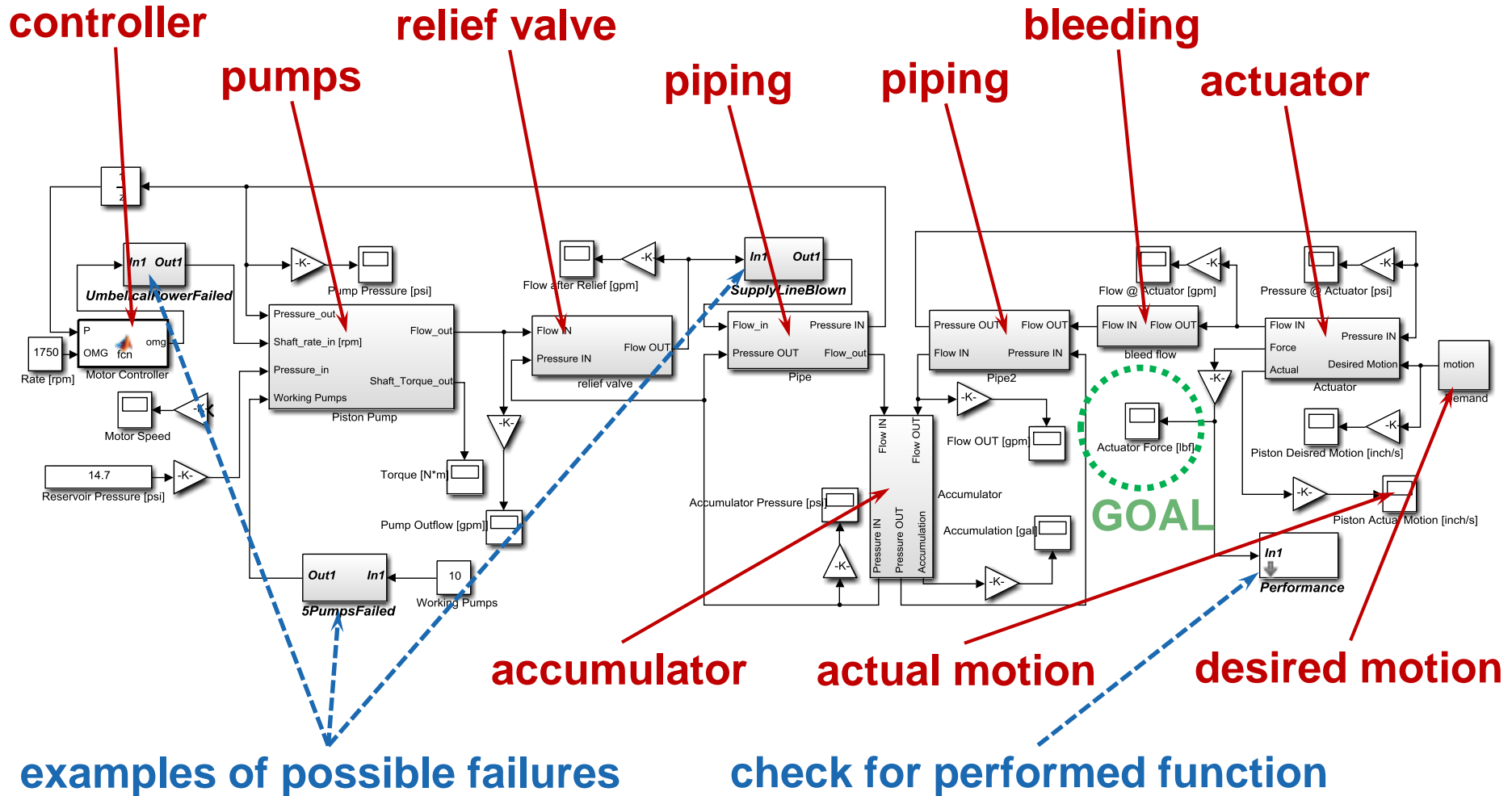
EXAMPLE

Example of Behavioral Model of Hydraulic Actuation

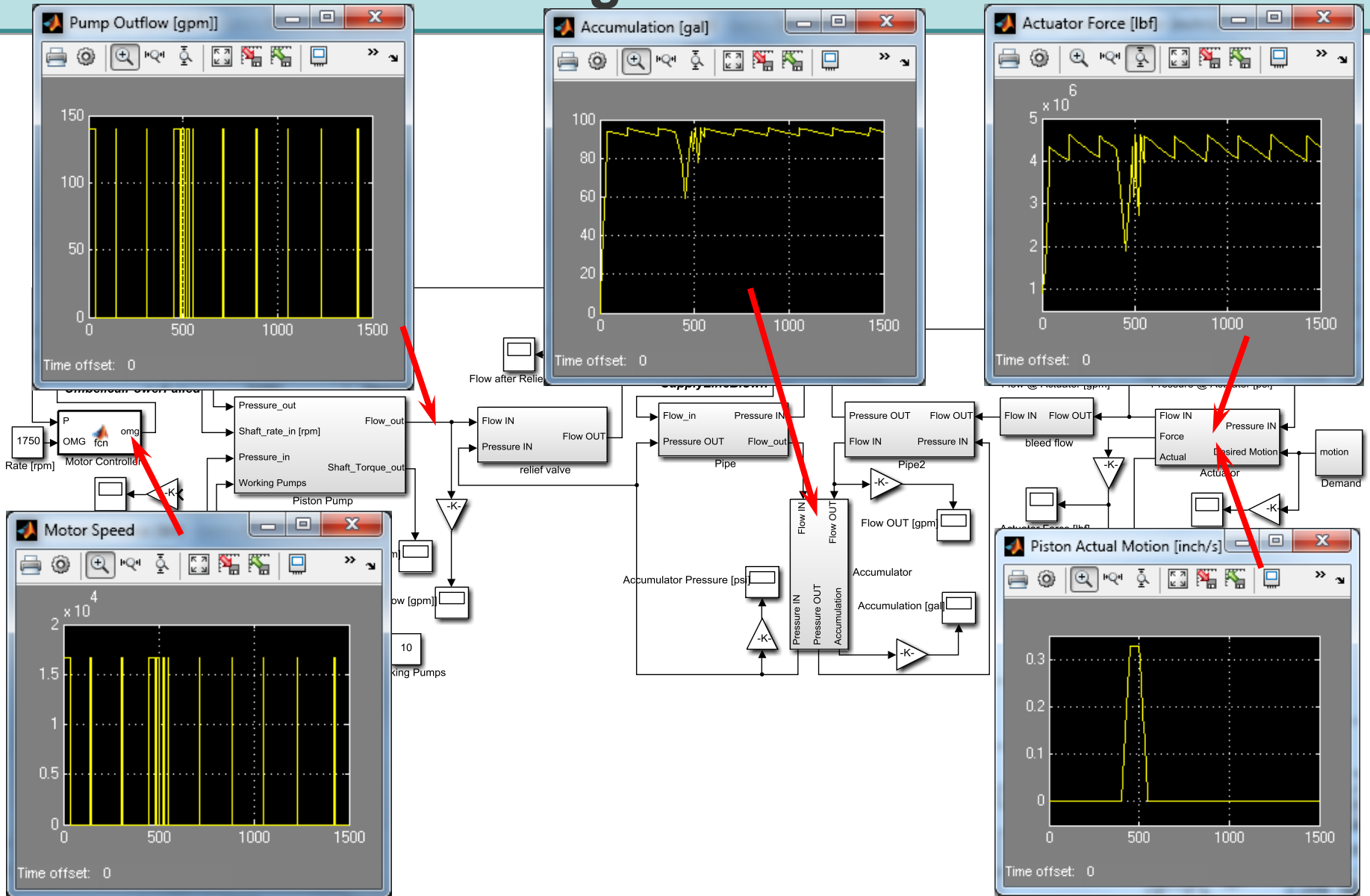


EXAMPLE

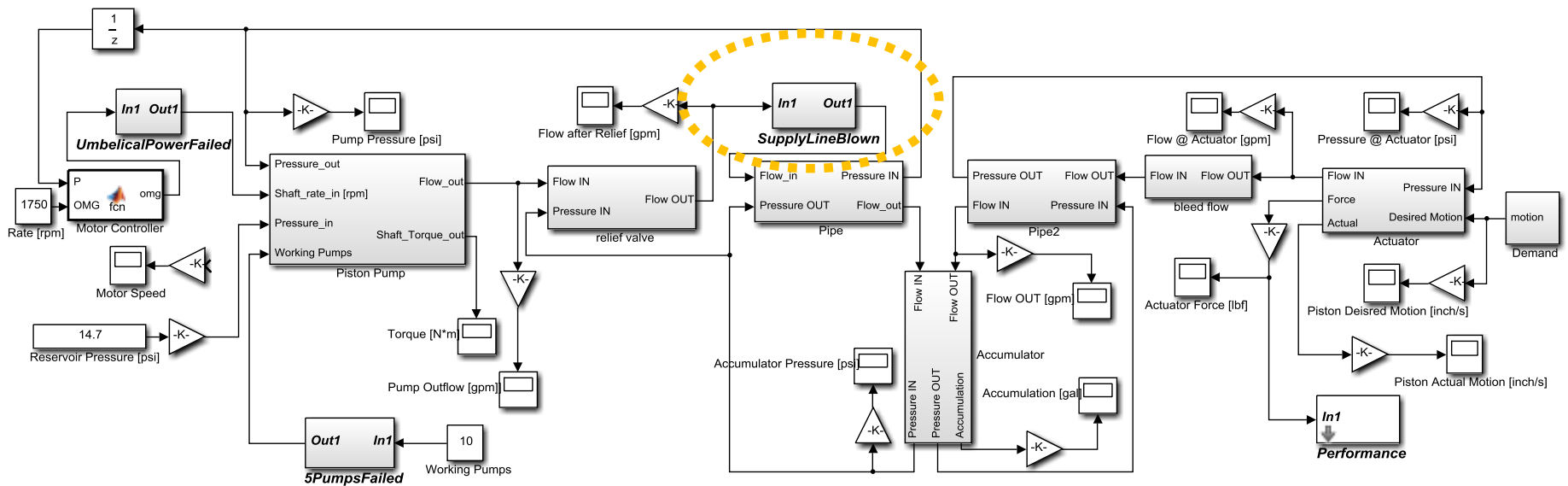
Behavioral Model of Hydraulic Actuation (cont'd)



Functioning Without Failures



Example of Functioning with a Failure

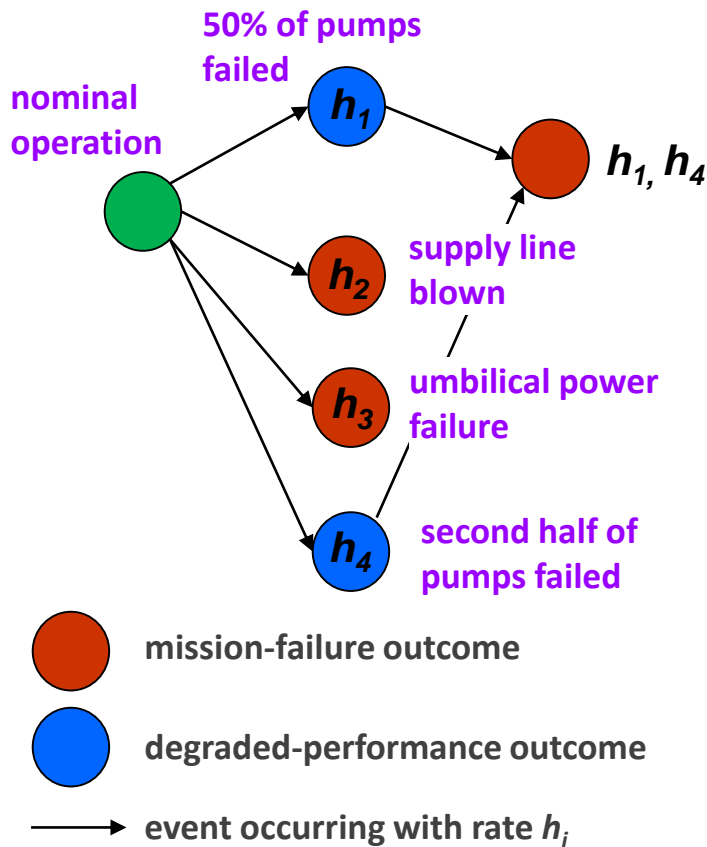


Example of Functioning with a Failure (cont'd)

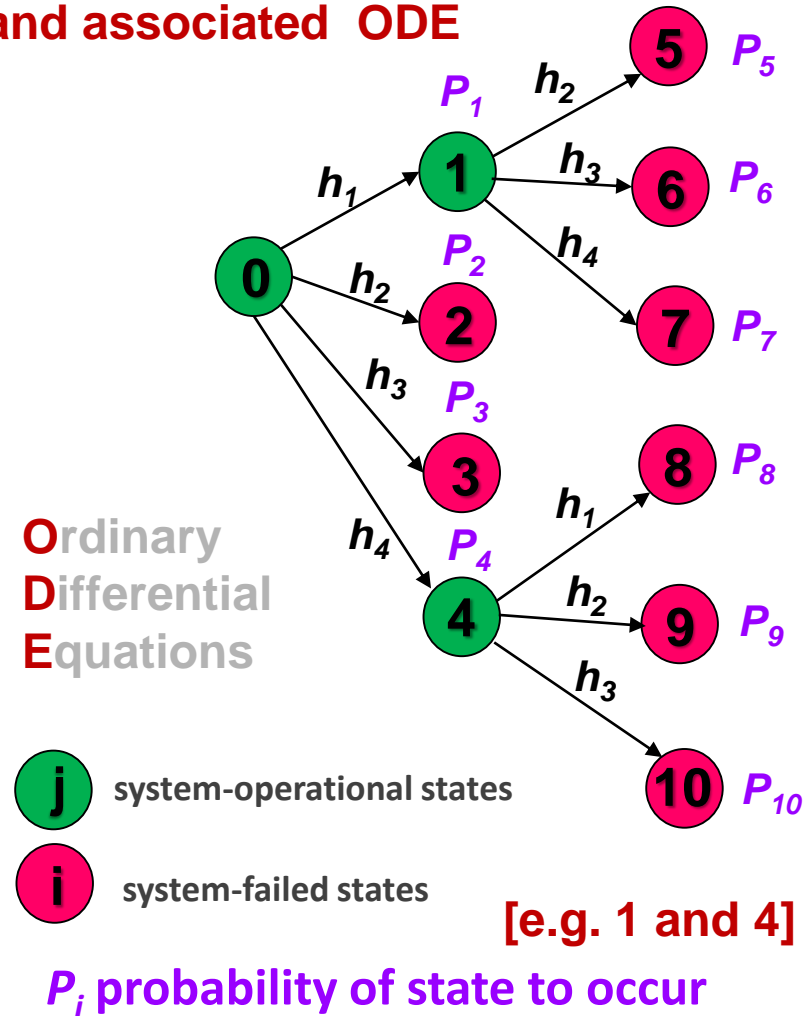


Simulations, Resulting Causal Network, and States

Simulation schedule: each circle is a mission simulation to identify all failures and operational states

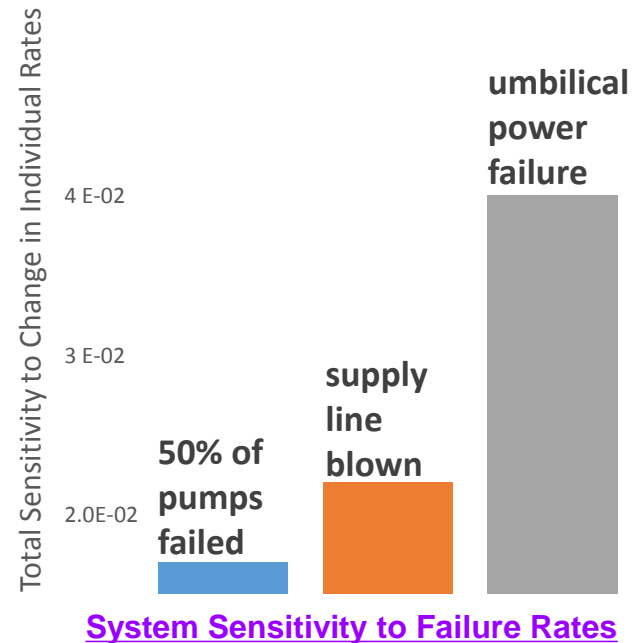
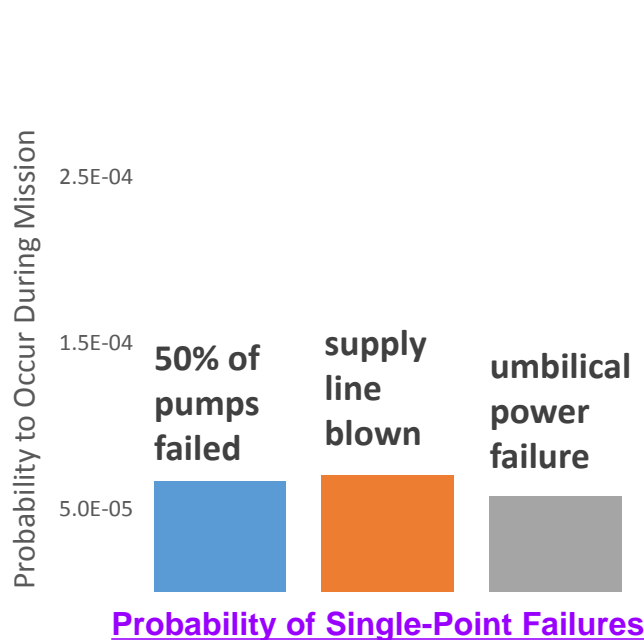


Related causal network and associated ODE



Reliability and Sensitivity Analysis

- Solution of ODE yields system reliability and whole system's sensitivity to individual failures



- Most sensitive failures call for higher modeling detail and process iterates until model is satisfactory and/or architecture is rendered fault tolerant (if so desired)

Networks and Associated ODEs

- The probability P_i of a state changes accordingly to the failure rates λ_j , repair rates μ_j , and probabilities P_j of the states connected to it
- As an example, for a case of a Markov chain, the equilibrium at the node would be as follows (cf. [3]):

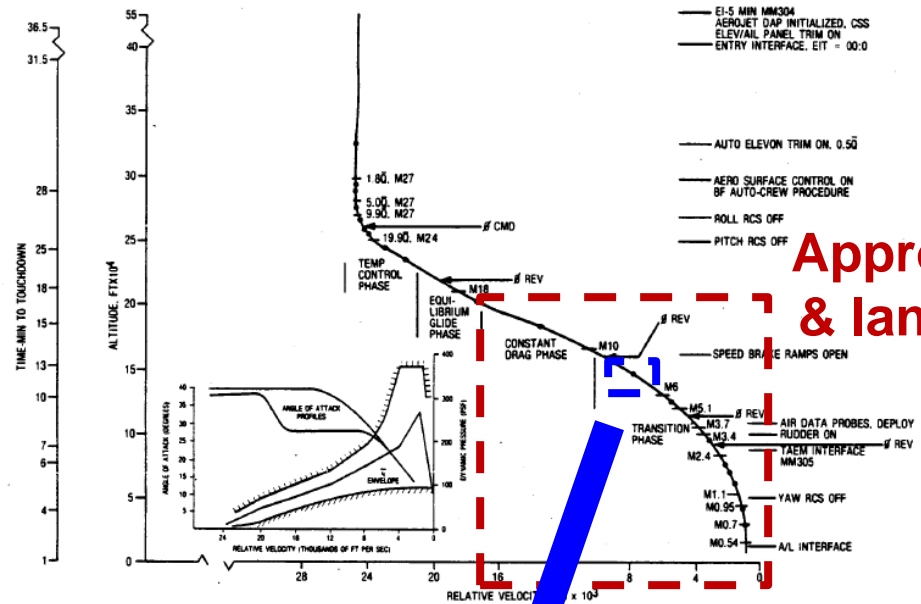
$$\frac{dP_i}{dt} = \sum_j \lambda_{j,i} P_j + \sum_q \mu_{q,i} P_q - \left(\sum_n \lambda_{i,q} + \sum_k \mu_{i,k} \right) P_i$$

- The ODE, so derived, allows for the calculation of P_i
- The concept can be applied to a general network; most applications result in Markov Chains
- Number of states and simulations can be from N to $\binom{N+1-1}{N-1}$, e.g., for N=100, failure states can be $10^2 - 10^5$

Man-in-the-Loop EXAMPLE

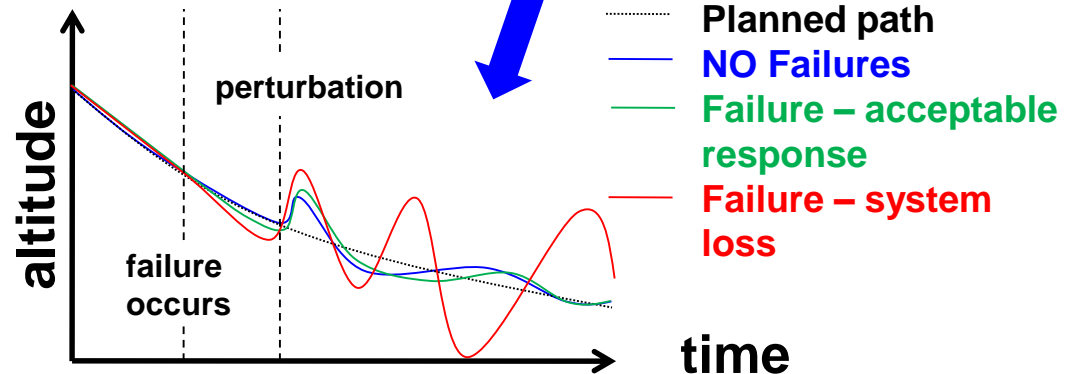
- Possible PoFs are:
 - Suboptimal control parameters
 - Pilot exhaustion causing PIOs
 - Pilot workload causing procedural error
 - Spacecraft damage
 - etc.

[cf. 4]



Approach & landing

Kafer, G.C. "Space Shuttle Entry / Landing Flight Control Design Description," 1982.



Model Update – Living Reliability Models

- Model-based RAPSODE allows for failure count prediction when a system or a family of products are in the field
- Therefore, as field data become available, the reliability model of the whole system or family can be tested and refined
- Unforeseen failure mechanisms will have different statistical signatures, which can be detected
- Different techniques, e.g., Bayesian, can be employed




Conclusions and Tasks for the Future

- Traditional component failures are used together with novel PoF models to capture complex interactions, phenomena, environment, human behavior, etc.
- Empirical and Analytical PoF models can be standardized and made into reusable libraries at the disposal of users
 - CFD, FEM, and similar analyses for subsystems and components
 - Models from legacy systems and data
 - Other
- Performance has been added as a proper reliability metrics in addition to system failure
- RAPSODE when used during the design phase drives laboratory testing



Conclusions and Tasks for the Future (cont'd)

- Simulation of all possible failure states can be very computationally and memory consuming but, at the present, this is no longer an issue 
- Techniques are available to manage “state explosion”
- Behavioral modeling is required by the methods
- Failure count for a family of products can be prospectively predicted and tracked starting from the design phase, thereby making cost of ownership a proper reliability metric in addition to system failure
- RAPSODE is a desirable expansion of Model-Based Engineering to integrate statistical reliability effects with functional performance modeling

Acknowledgments

The author thanks all esteemed colleagues, not limited to Mr. Jeffrey J. Zinchuck, whose contributions have inspired RAPSODE, and Mr. Marvin A. Biren for his suggestions based on a life-long experience in system engineering of complex one-of-a-kind systems.

A particular acknowledgment goes to Mr. Walter D. Clark for his extensive contribution to the statistical methods.

References

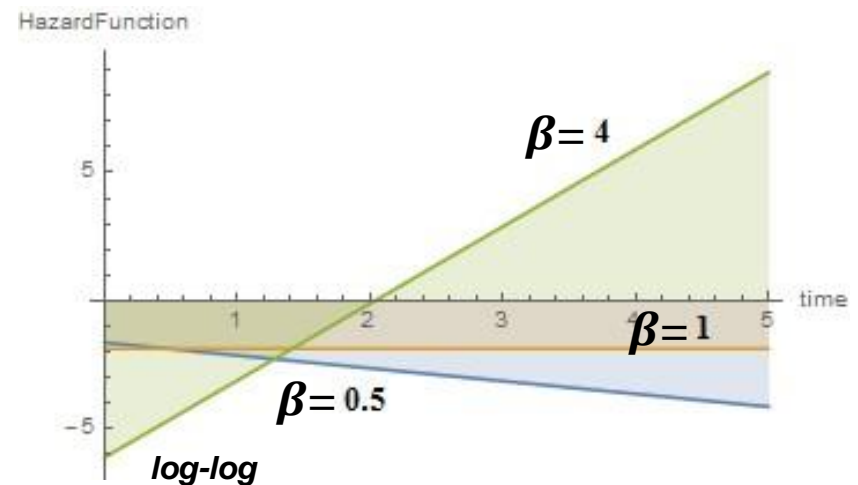
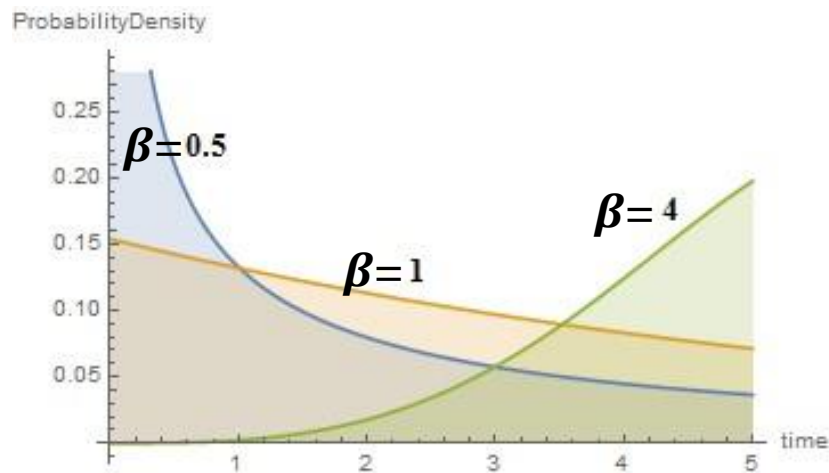
- [1] Borer, N., I. Claypool, D. Clark, J. West, K. Somerville, R. Odegard, N. Suzuki, “Model-Driven Development of Reliable Avionics Architectures for Lunar Surface Systems,” *IEEEAC paper #1568*, January 5, 2010.
- [2] Agte, J.S., N.K. Borer, O. de Weck, “A Simulation-Based Design Model for Analysis and Optimization of Multi-State Aircraft Performance,” 51st AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Material Conference, 12-15 April 2010, Orlando Florida.
- [3] World Wide Web source: <http://www.mathpages.com/home/index.htm>
- [4] Bortolami, S.B., K.R. Duda, N.K. Borer, “Markov Analysis of Human-in-the-Loop System Performance,” IEEE Aerospace Conference, Big Sky, MT, March 2010.
- [5] Babcock IV, P.S., J.J., Zinchuk, “Fault-Tolerant Design Optimization: Application to an Autonomous Underwater Vehicle Navigation System,” The Charles Stark Draper Laboratory, Inc., Cambridge, MA. *Proceedings of the (1990) Symposium on Autonomous Underwater Vehicle Technology*, 1990.
- [6] Savage, M., K.C. Radil, D.G. Lewicki, J.J. Coy, “Computerized Life and Reliability Modeling for Turboprop Transmissions,” *J. Propulsion and Power*, Vol. 5, No. 5, 1989, pp. 610-614.
- [7] McLeish, J.G., “Enhancing MIL-HDBK-217 Reliability Predictions with Physics of Failure Methods,” *Proceedings of the IEEE, Reliability and Maintainability Symposium (RAMS)*, San Jose, CA, 2010, pp. 1-6.

Useful Probability Definitions

- $F(t)$ is the probability of an “event,” i.e., failure, to occur by a given time (Cumulative Distribution Function, or CDF)
- $f(t)=dF(t)/dt$, is the Probability Density Function (PDF) of the failure event with respect to time
- $R(t)=1-F(t)$ is the reliability function or the residual probability of the event not to occur by a given time
- $h(t)=f(t)/R(t)$, called the ***hazard function***, is the PDF of the failure event *given that the item has survived to time t .*

Reliability Using Weibull Statistics

$$F(t) = 1 - e^{-\left(\frac{t}{\alpha}\right)^\beta} \quad \text{and} \quad h(t) = \frac{\beta}{\alpha} \left(\frac{t}{\alpha}\right)^{\beta-1} \quad \text{for } t > 0$$



- $\beta < 1$ indicates a decreasing failure rate or infant mortality failure type
- $\beta = 1$ indicates a constant failure rate
- $\beta > 1$ indicates an increasing failure rate or a wear-out failure type

Special Case – Constant Failure Rate

$$F(t) = 1 - e^{-\lambda t} \quad \text{and} \quad h(t) = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \quad \text{for } t > 0$$

PRACTICAL REMARKS:

- ✓ Constant Failure Rate is commonly used in reliability engineering
- ✓ λ Represents failures per unit of time, e.g., 10^{-9} [h⁻¹]
- ✓ $1/\lambda$ Is the MTBF, e.g., 10^9 [h]
- ✓ *MTBF* By this time, half of the units are expected to have failed
- ✓ $\lambda_{Tot} = \sum \lambda_i$ Is the failure rate of a system of i components



THANK YOU