COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

Modeling Trust in Critical Systems with Möbius

KEN KEEFE
SENIOR SOFTWARE ENGINEER
LEAD MOBIUS DEVELOPER

ITI.ILLINOIS.EDU

INFORMATION TRUST INSTITUTE

Course Overview

- Objective: Give course attendees an intense introduction to modeling systems using Mobius, stochastic activity networks, and ADversary VIew SEcurity models. Provide enough background so that they can begin evaluating the availability, reliability, performability, and security of their system designs by the end of the course.

- Prerequisites:

  - Undergraduate course in probability and statistics

  - Basic knowledge of C++ syntax

- Much of the course will be hands-on, with the instructor providing individual help on modeling with SANs and Mobius. The exercises will relate to a variety of different types of design.

Session Outline

- Introduction
- Modeling Introduction
- Mobius Overview
- Building Models in Mobius
  - Stochastic Activity Networks
  - Replicate/Join Models

Attendee Introduction

- Name
- Background
- Current Work
- Why are you taking the course?

System Validation

- **Valid** - Able to effect or accomplish what is designed or intended
- Two Notions
  - **Specification** - A description of what a system is supposed to do.
  - **Realization** - A description of what a system is and does.
- **Validation** - the process of determining whether a realization meets its specification.
- In this class, the specification is expressed in terms of *performance/dependability/security measures* and the realization is a *system model* in Mobius.

System Validation

- **Measures** - What you want to know about a system. Used to determine if a realization meets a specification
- **Models** - Abstraction of the system at an appropriate level of abstraction and/or details to determine the desired measures about a realization.
- **Model Solution Methods** - Method by which one determines measures from a model. Models can be solved by a variety of techniques:
  - **Combinatorial Methods** - Structure of the model is used to obtain a simple arithmetic solution.
  - **Analytical/Numerical Methods** - A system of linear differential equations or linear equations is constructed, which is solved to obtain the desired measures
  - **Simulation** - The realization of the system is executed, and estimates of the measures are calculated based on the resulting executions (known also as *sample paths* or *trajectories*.)
- Mobius supports performance/reliability/availability validation by analytical/numerical and simulation-based methods.

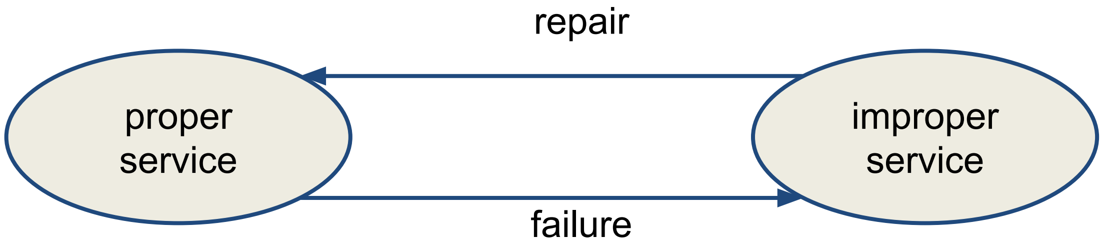
What's a System?

- Many things, but in the context of this class, a collection of
  - Hardware
  - Networks
  - Operating Systems
  - Application Software

  that is intended to perform according to some specification.
- The specification can relate to the system's
  - Dependability (e.g., availability and reliability)
  - Performance (e.g., response time)
  - Performability (e.g., response time in the presence of faults).

Dependability

- **Dependability** is the ability of a system to deliver a specified service.
- System service is classified as **proper** if it is delivered as specified; otherwise it is **improper**.
- System **failure** is a transition from proper to improper service.
- System **restoration** is a transition from improper to proper service.



The *properness* of service depends on the user's viewpoint!

Reference: J.C. Laprie (ed.), Dependability: Basic Concepts and Terminology, Springer-Verlag, 1992.

Availability

Quantifies the alternation between deliveries of **proper** and **improper** service.

- A(t) is 1 if service is proper at time t, 0 otherwise.
- E[A(t)] (Expected value of A(t)) is the probability that service is proper at time t.
- A(0,t) is the fraction of time the system delivers proper service during [0, t].
- is the expected fraction of time service is proper during [0,t].
- $E[A(0,t)]$ is the probability that service is proper more than 100t*% of the time during [0,t]. $P[A(0,t) > t^*] (0 \le t^* \le 1)$
- is the fraction of time that service is proper in steady state.
- $A(0,t)_{t\rightarrow\infty}$ as above.

$E[A(0,t)_{t\rightarrow\infty}], P[A(0,t)_{t\rightarrow\infty} > t^*]$

Other Dependability Measures

- **Reliability** - a measure of the continuous delivery of service
  - R(t) is the probability that a system delivers proper service throughout [0,t].
- **Safety** - a measure of the time to catastrophic failure
  - S(t) is the probability that no catastrophic failures occur during [0,t].
  - Analogous to reliability, but concerned with catastrophic failures.
- **Time to Failure** - measure of the time to failure from last restoration. (Expected value of this measure is referred to as **MTTF - Mean time to failure.**)
- **Maintainability** - measure of the time to restoration from last experienced failure. (Expected value of this measure is referred to as **MTTR - Mean time to repair**.)
- **Coverage** - the probability that, given a fault, the system can tolerate the fault and continue to deliver proper service.

Performance

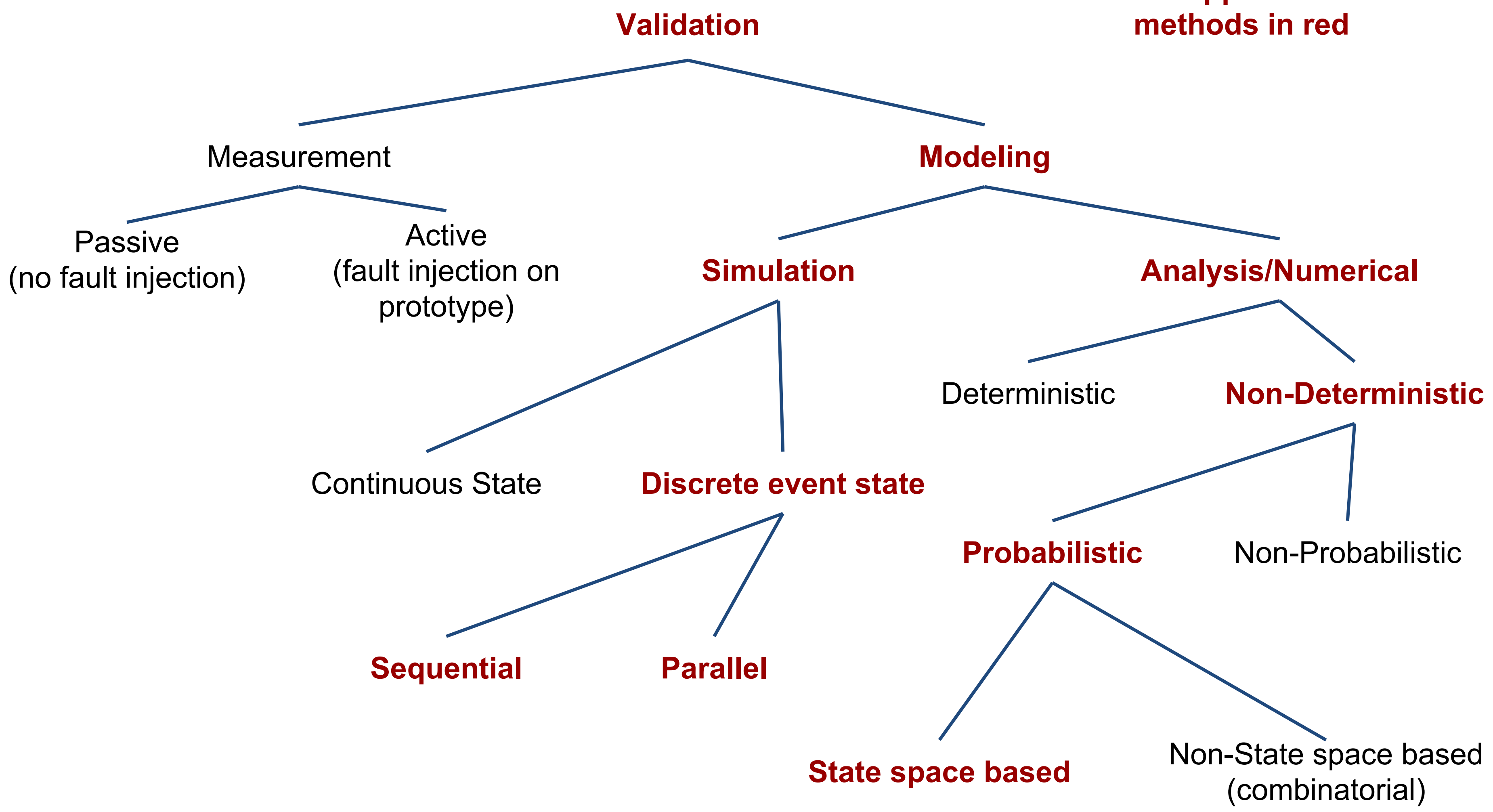
- **Performance** - how well a system performs, provide that service is proper
- Example (Generic) Performance Measures:
  - **throughput** - the number of jobs processed per unit time
  - **response time** - the time to process a specific job
  - **capacity** - the maximum number of jobs that may be processed per unit time
- Most practical performance measures are very application specific, and measure times to perform particular functions or, more generally, the probability distribution function of the time to perform a function.

Performability

- **Performability** quantifies how well a system performs, taking into account behavior due to the occurrence of faults.
- It generalizes the notion of dependability in two ways:
  - includes performance-related impairments to proper service.
  - considers multiple levels of service in specification, possibly an uncountable number.
- Performability measures are truly user-oriented, quantifying performance as perceived by users.

Validation Methods

Mobius supported methods in red



Validation

Measurement

Passive (no fault injection)

Active (fault injection on prototype)

Modeling

Simulation

Continuous State

Discrete event state

Sequential

Parallel

Analysis/Numerical

Deterministic

Non-Deterministic

Probabilistic

Non-Probabilistic

State space based

Non-State space based (combinatorial)

Model Solution Issues

- In general:
  - Use *tricks* from probability theory to reduce complexity of model
  - Choose the right solution method
- Simulation
  - Result is just an estimator based on a statistical experiment
  - Estimation of accuracy of estimate essential
  - Use confidence Intervals!
- Analytical/Numerical model solution
  - Avoid state space explosion
    - Limit model complexity
    - Use structure of model (symmetries) to reduce state space size
  - Understand accuracy/limitations of chose numerical method
    - Transient Solution
    - (Iterative or Direct) Steady-state solution

Model Solution Issues

- There is no single or definitive source; input parameter values for a model depend on the environment and nature of the system being designed.
- Often, parameter values must come from experiments performed on the system itself (via fault injection)
- However, there are several sources for failure information, including:
  - Military Handbook: Reliability Prediction of Electronic Equipment (MIL-HDBK-217F, 2 December 1991)
    - Failure rates often expressed in “FITS” - failures per 109 hours.
  - Westinghouse Electric Corporation Reliability Analysis/Assessment of Advanced Technologies (RADC-TR-90-72, May 1990)
    - Examines existing failure rate models in microcircuit section of MIL-HDBK-217E to determine whether they are applicable to state-of-the-art devices.

Model Construction

- Understand the desired measure before you build the model.
- The desired measure determines the type of model and the level of detail required. No model is universal!
- Steps in constructing a model:
  a. Choose the desired measures:
     - Choice of measures form a basis for comparison.
     - It's easy to choose wrong measure and see patterns where none exist.
     - Measures should be refined during the design and validation process.

  b. Choose the appropriate level of detail/abstraction for model components.
     - Key is to represent model at the right level of detail for the chosen measures.
     - It is almost never possible or practical to include all system aspects.
     - Model the system at the highest level possible to obtain a good estimate of the desired measures.

  c. Build the model.
     - Decide how to break up the model into modules, and how the modules will interact with one another.
     - Test the model as you build it, to ensure it executes as intended.

Model Solution

- Use the appropriate model solution technique:
  - Just because you have a hammer doesn’t mean the world is a nail.
  - There is no universal model solution technique (not even simulation!)
  - The appropriate model solution technique depends on model characteristics.
- Use representative input values:
  - The results of a model solution are only as good as the inputs.
  - The inputs will never be perfect.
  - Understand how uncertainty in inputs affects measures.
  - Do sensitivity analysis.
- Include important points in the design/parameter space:
  - Parameterize choices when design or input values are not fixed.
  - A complete parametric study is usually not possible.
  - Some parameters will have to be fixed at *nominal* values.
  - Make sure you vary the important ones.

Model Interpretation/Documentation

- Make all your assumptions explicit:
  - Results from models are only as good as the assumptions that were made in obtaining them.
  - It's easy to forget assumptions if they are not recorded explicitly.
- Understand the meaning of the obtained measures:
  - Numbers are not insights.
  - Understand the accuracy of the obtained measures, e.g., confidence intervals for simulation.
- Keep social aspects in mind:
  - Performance and dependability analysts almost always bring bad news.
  - Bearers of bad news are rarely welcomed.
  - In presentations, concentrate on results, not the process.