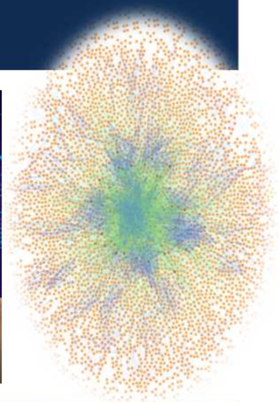
SAND2016-6116PE



Enabling V&V for Engineered Complex Systems via Resilient Design

Jackson Mayo, Sandia/California

June 22, 2016

Workshop on Complex Systems Models and Their Applications: Towards a New Science of Verification, Validation and Uncertainty Quantification

Sandia National Laboratories

Exceptional service in the national interest

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Mathematics shows the limits of understanding complex systems

- Complex systems behave as large-scale information networks
- Theorem (Turing 1936, Rice 1953): **No algorithm exists** to predict a priori the behavior of a **generic** information processing system
  - i.e., such a system is **undecidable** (in the limit) even if **deterministic**
  - A real system, with a **finite exponentially large** number of states but **otherwise generic**, is *effectively* undecidable – in particular, testing/simulation cannot bound its behavior beyond the scenarios actually tested/simulated

?

The theory has direct V&V and UQ implications

- A complex system *created arbitrarily* cannot be predicted or bounded
  - You have **no idea** how the system, or the model, will respond in the vast number of scenarios you **haven't** tested
  - Once the state differs even slightly from what you expected – due to a modeling error, a natural fault, or an attack – all bets are off
- Yet, why do **some** complex systems seem to exhibit predictable behavior with quantifiable reliability/uncertainty?
  - e.g., many biological and social systems
  - Hint: These systems have **evolved** and possess inherent **resiliency** properties
  - How can we leverage similar properties for engineered systems?

Area for research: What makes resilient complex systems quantifiable?

- Smoothness (a.k.a. stability, subcriticality) makes a system:
  - **Predictable** (you can extrapolate its behavior to a new situation)
  - **Resilient** (it tends to maintain its behavior under minor faults)
  - **Evolvable** (you can make small changes to it, and it remains usable)
- Smoothness *of particular observables* is common in physics
  - Amid molecular chaos, continuum equations apply when we're concerned with thermodynamic (averaged) behavior
  - Extend this to **adaptive** complex systems *with respect to the behaviors that are selected for?* (These are typically **not** averaged behaviors)
- Ability to bound the effect of **perturbations** is crucial for:
  - Inferring that a model will be predictive under conditions that **differ** from those used to test it (**V&V**), and inferring how much the model behavior may change due to **variations** in input parameters (**UQ**)

A lesson for complex systems that are *not* resilient

- Beware of applying techniques that assume smoothness/ stability to complex system observables that have no reason to be smooth/stable
  - Could be garbage in, garbage out
- Today's complex **digital** systems are **not** designed in a thoroughly adaptive way, and lack inherent stability
  - Hence, highly susceptible to failures and attacks
  - By the same token, also difficult to model predictively
- The *difficulty of V&V'ing cyber(-physical) models* and the *difficulty of securing cyber(-physical) systems* are two sides of the same coin
  - The cyber V&V problem **is** the cybersecurity problem – both need to be solved together