STEAM INTELLIGENCE

Prediction Has Limits:

Bridging the Model–Measurement Boundary

A structured educational guide exploring models, measurements, and physical artificial intelligence.

Presented by Dr. Albert Tan Lie Sing

Mathematical Physicist • AI Robotics Systems Architect • STEAM Education Innovator

Omitted variables can mislead real physical decisions

The Selection Bottleneck

• Selection Inevitability: Every scientific or computational model must select a subset of reality to represent. It chooses what variables, relationships, boundaries, and scales to include.

• Hidden Exclusions: This deliberate selection process inherently determines what remains entirely outside of the model's explanation.

• The Validity Risk: A model can be perfectly internally consistent, elegant, and mathematically sound, and yet still completely mislead a real-world physical decision.

Consequences of Omitted Interactions

• Classical Pendulum: Traditional introductory physics equations describe small swings of a pendulum, but completely omit how larger swings are dependent on amplitude.

• AI Robotics Sim-to-Real: Simulators represent physical motion but regularly simplify surface friction, sensor behaviors, or control feedback delays.

• The Practical Question: The issue is not that models simplify; it is whether the omitted physical interactions change the downstream decision we are making.

Unscrutinized sensors introduce hidden systematic bias

Scrutinizing Measurement Limits

• Precision vs. Accuracy: A finely resolved instrument display with more decimal places does not establish accuracy. Repeatability-related precision is distinct from absolute correctness.

• Invisible Systematic Bias: Repeated readings can cluster tightly yet share the exact same systematic offset. Averaging more measurements will never remove this offset.

• The Interface Gap: Before assuming a model is incorrect when it disagrees with a sensor, we must scrutinize what, where, and when the sensor actually measured.

Conflating System Verification & Validation

• The Conflation Hazard: Project teams often confuse math verification, parameter calibration, and physical validation. They treat code execution agreement as real-world proof.

• Calibration Compensation: Tuning model parameters to fit historical data can mask physical omissions. The model matches a narrow reference range but fails when generalized.

• The Metrology Misalignment: A physical sensor measures casing temperature, while the model predicts internal motor core temperature. Treating these as interchangeable creates a major gap.

Three core objectives establish validation discipline

1. Build Bounded Claims

Move away from open-ended, absolute assertions of performance.

Ensure every model prediction is accompanied by a bounded, rigorous statement of:

- What specific task was tested
- The precise environmental conditions
- The explicit success criteria used
- The documented remaining uncertainty

2. Drive Intentional Revision

Treat model-measurement disagreement not as a failure, but as a rich scientific prompt.

This forces stakeholders to:

- Mathematically explain discrepancies
- Systematically challenge assumptions
- Design targeted trials that force model revision or restrict its operational scope

3. Evaluate Contextual Risk

Implement continuous evaluation at operational boundaries.

Aligning with NIST frameworks to manage physical AI safely, we must:

- Map out-of-scope conditions (wear, shifts)
- Formulate requirements for human safety intervention
- Establish lifecycle monitoring protocols

NASA's standard separates verification and validation

SYSTEM VERIFICATION

"Does the code match the math?"

Focus: Conformity to Specifications

- Ensures that the calculations faithfully implement the underlying mathematical equations.
- Checks software and mathematical correctness.
- Warning: A calculation can perfectly conform to a model that is completely unsuitable for the physical task.

MODEL CALIBRATION

"Can we tune the model to fit?"

Focus: Parameter Optimization

- Adjusts model parameters against a chosen set of historical reference data.
- Maximizes curves to fit known physical experiments.
- Warning: Parameters can compensate for entirely omitted physical effects over a narrow, convenient fitting range.

SYSTEM VALIDATION

"Does the model match reality?"

Focus: Representation for Intended Use

- Evaluates how adequately the model represents the physical system for its intended real-world task.
- Requires testing against reserved, out-of-fit data.
- Success: Earns a bounded credibility claim with explicitly documented uncertainty limits.

The physical pendulum reveals finite amplitude limits

Mathematical Model and Simplification

• The Ideal Model: For an ideal point mass suspended by length L, uniform gravity g, and negligible friction, the period is described by the simple pendulum equation:

$$T_0 = 2\pi\sqrt{(L/g)}$$

• The Omission: This model replaces $\sin\theta$ with θ. It assumes the swing amplitude is so small that θ is roughly equivalent to its sine.

• Dimensional Consistency: L/g has units of seconds squared, so its square root matches the dimension of time (seconds). However, mathematical consistency does not guarantee physical accuracy.

Reality Check: Amplitude Dependence

• Finite Amplitude Correction: When a pendulum swings at a larger angle θ_0, its period increases. The leading relative correction to the period is:

$$\text{Relative Correction} = \theta_0^2 / 16$$

• The Boundary Revealed: For small swings (e.g., 0.1 rad), the error is negligible (less than 0.1%). But for a larger swing (e.g., 1.0 rad), the period increases by ~6.25%, making the simple model inaccurate.

• The Lesson: This does not make the introductory model useless. Instead, it defines the clear boundaries under which the model's simplifications remain acceptable.

Robotics studies prove transfer requires variation

1. AI Robotics Sim-to-Real Experiments

• Tobin et al. (2017) Object-Localization Networks: Trained deep neural networks in 3D simulation. They found that omitting visual distracting objects in simulation critically impaired physical localization when the robot faced distractors in real-world test scenes.

• Peng et al. (2018) Sim-to-Real Transfer: Successfully transferred a learned puck-pushing controller to a physical robot. Their experiments showed that varying physical dynamics and timings (dynamics randomization) during simulation training was absolutely necessary to avoid physical transfer failures.

2. Deterministic Chaos and Forecast Horizons

• Lorenz (1963) Flow Model: Edward Lorenz demonstrated extreme sensitivity to starting states in a simplified atmospheric deterministic model.

• Exponential Divergence: Tiny differences in initial states (well below measurement resolution) grow exponentially over time.

• The Absolute Horizon: This sensitive dependence sets a strict mathematical limit on long-term detailed predictions, proving that even fully deterministic, well-specified physical systems lose trajectory support over time.

Changed environments demand continuous re-evaluation

Model Validation Limitations

• Validation is Bounded: Validation never proves a model is 'correct.' It earns a strictly bounded statement of what was tested, under what conditions, and with what remaining uncertainty.

• Distribution Shift: Change in environmental conditions, operational requirements, or hardware wear can instantly invalidate previous validation results.

• Forecast Horizons: Under chaotic dynamics, long-term trajectory predictions are fundamentally impossible; we must restrict our predictions to defined horizons.

Conclusion: Ongoing Risk Management

• Continuous Monitoring: NIST's 2023 AI Risk Management Framework (AI RMF) connects evaluation to realistic use and ongoing real-world monitoring.

• Triggers for Re-evaluation: We must treat changed physical hardware, new operating environments, and revised requirements as immediate reasons to revisit model assumptions.

• Credibility Formula: A prediction's credibility rests on a clear, documented relationship among active assumptions, physical measurements, and decision consequences.

Four fundamental questions expose what was left out

THE SHARED DISCIPLINE OF SCIENTIFIC INQUIRY

What Did We Leave Out?

To put these insights into practice, every research team, classroom, and organization should confront four fundamental questions before acting on any prediction:

1. *What is being predicted, and on what exact timescale does its accuracy matter? [Passage 14, 26]*
2. *What was actually measured, and does its timing, location, and unit match our model's quantities? [Passage 10, 26]*
3. *Which environmental conditions were explicitly tested, and which remain entirely unknown? [Passage 12, 30]*
4. *What specific, observed evidence would make us revise the model or restrict its use? [Passage 4, 30]*

"The credibility of a prediction depends on how clearly we can explain its limits." — Dr. Albert Tan Lie Sing