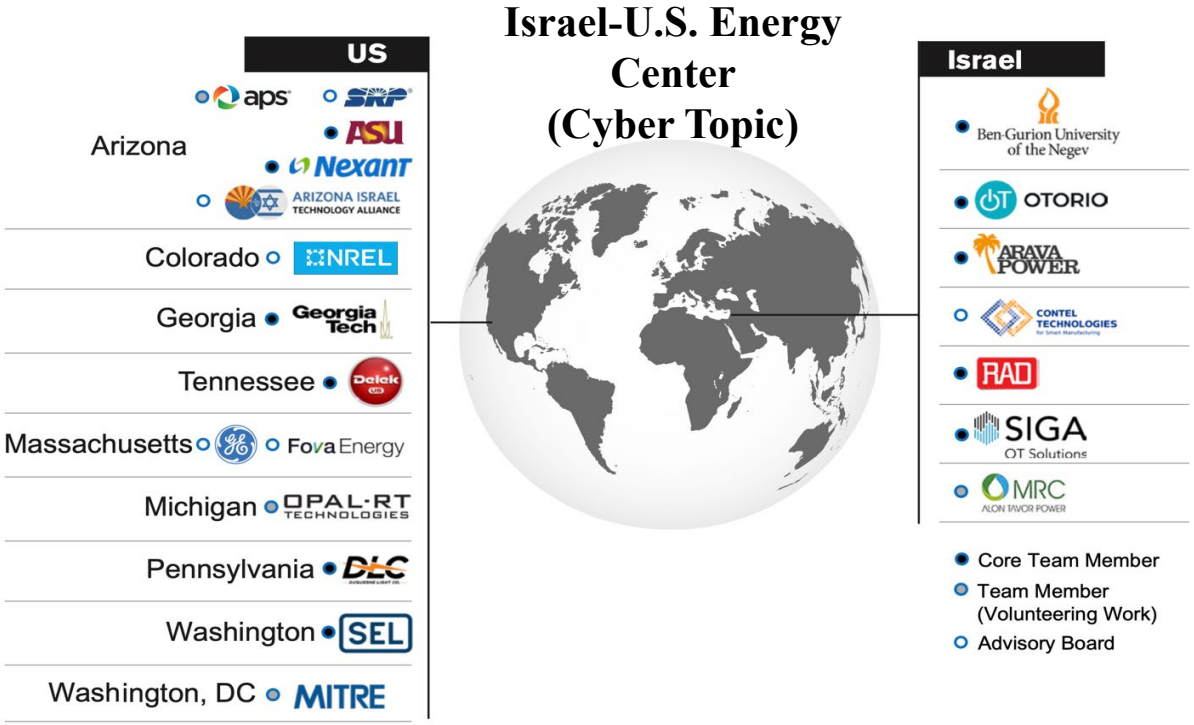
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Prepared for

Itai Ganzer and **Ofer Goldhirsh**

Israel Innovation Authority

Avi Shavit and **Eynan Lichterman**

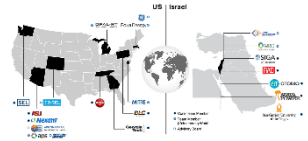
Israel Ministry of Energy

Task 11: AI Based Intrusion Detection

Ling-Wei Kong
on behalf of
Ying-Cheng Lai
Arizona State University

8/25/2022

Digital Twins for Intrusion Detection



- Predict the dynamical response of a nonlinear cyberphysical system under:

❑ parameter drift

❑ unseen driving signals

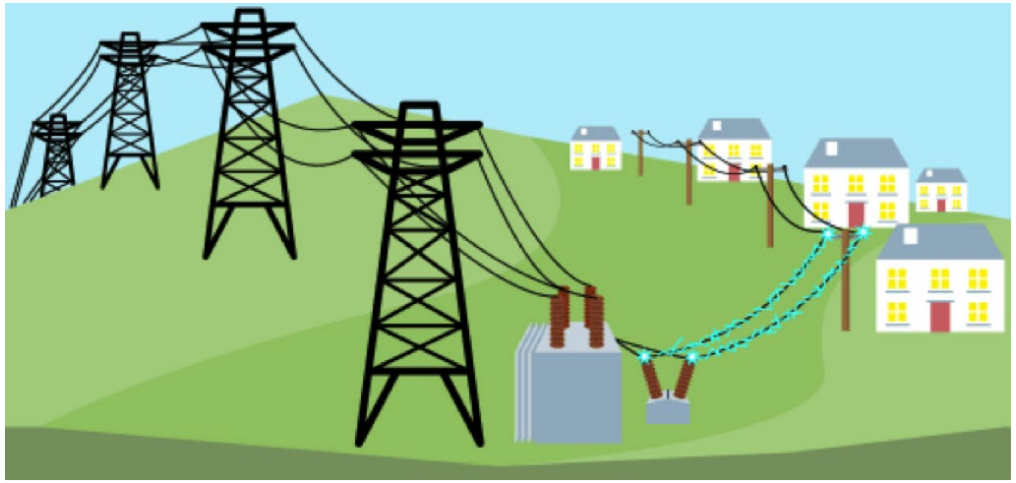
- anticipation of possible qualitative changes caused by dynamical bifurcations

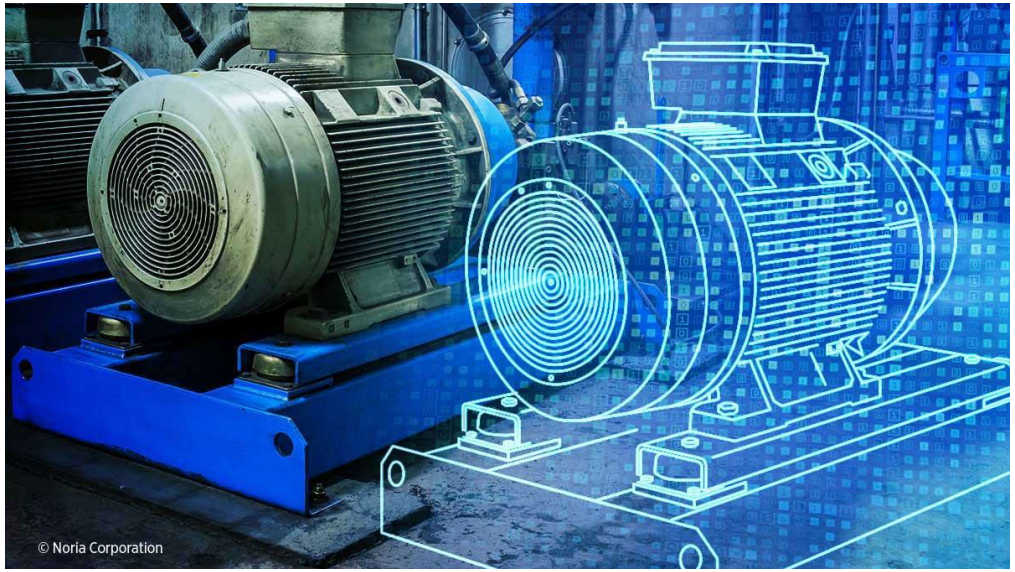
- Real-time situation awareness with sparse updates

❑ in-time monitoring of hidden variables with partial and temporally sparse observations

❑ continual forecasting of the observables and hidden variables with partial and temporally sparse observations

- …

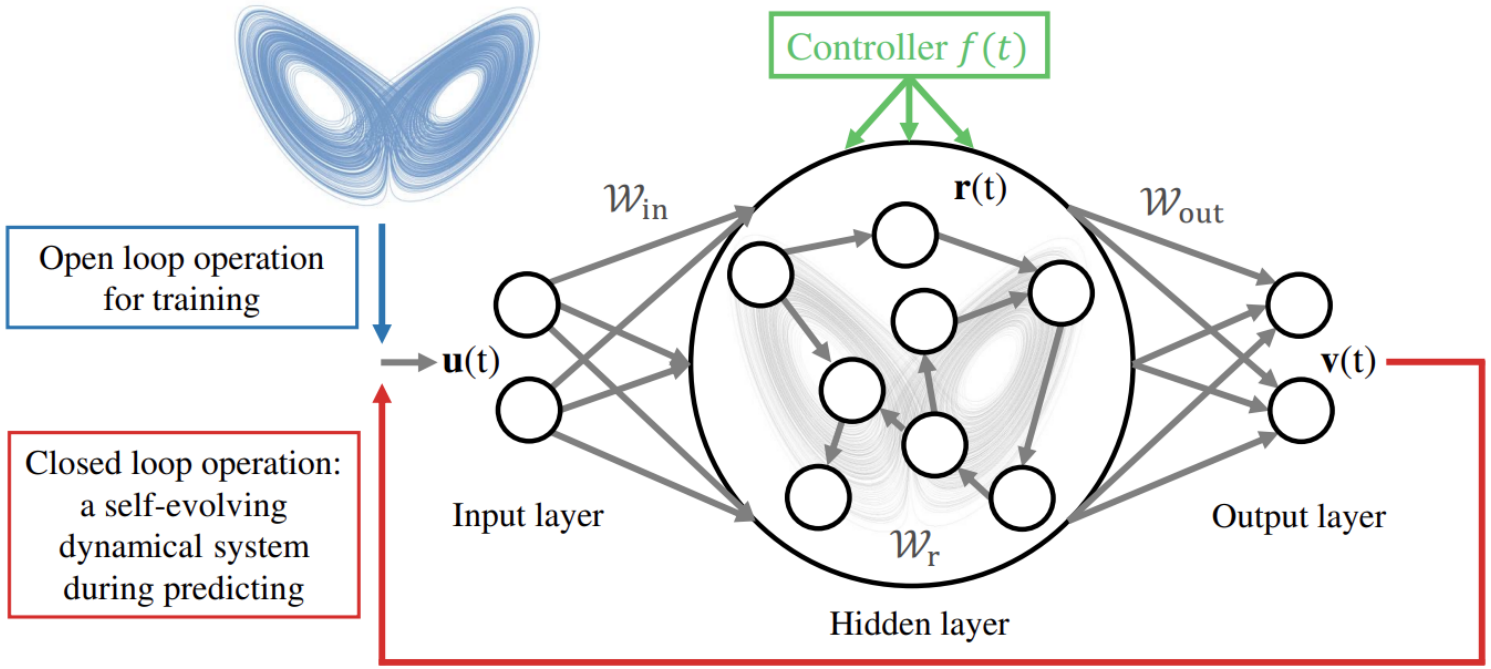




These requirements for a reliable digital twin becomes especially difficult when:

- the system is **nonlinear**
- the system is **high-dimensional**

Machine Learning Architecture: Adaptable Reservoir Computing

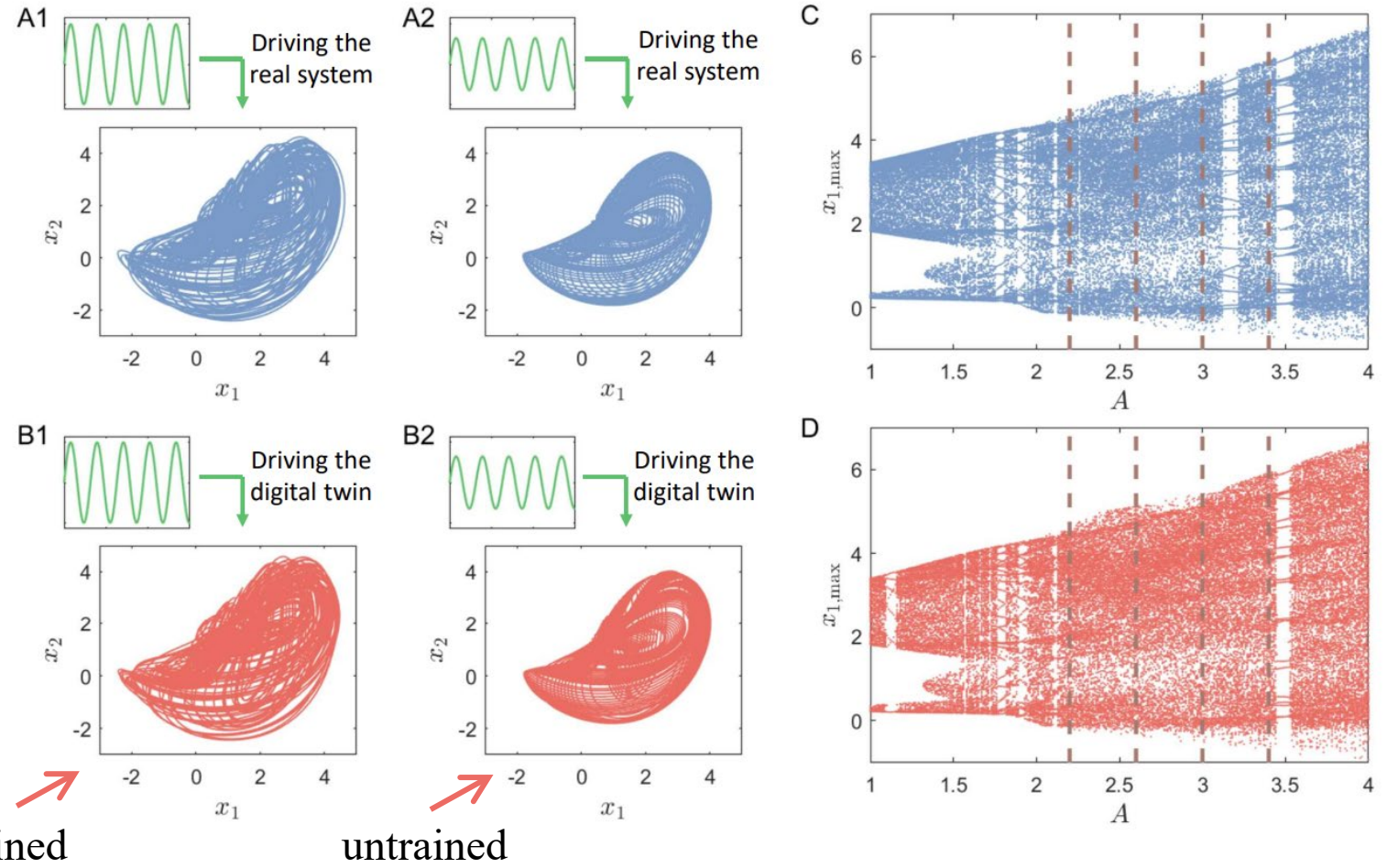


Predicting Dynamical Behaviors and Bifurcations

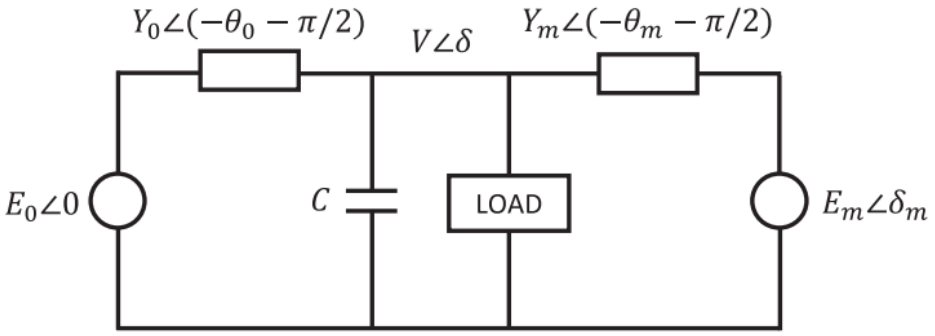
Lorenz-96 system $\frac{dx_k}{dt} = x_{k-1}(x_{k+1} - x_{k-2}) - x_k + f(t), \quad k = 1, 2, \ldots, 6$

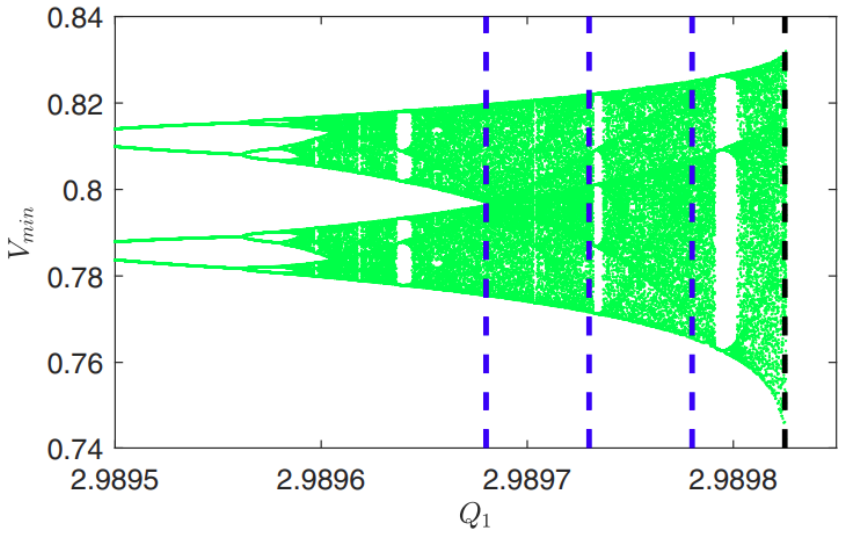
blue: results with the ODE model

red: results with the digital twin

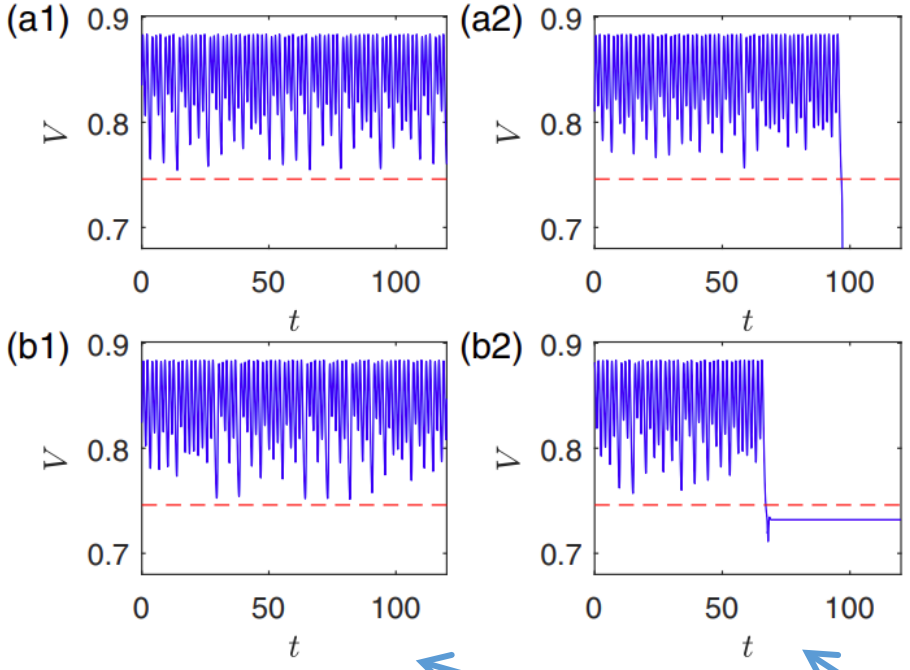


Anticipating Power System Collapse





true dynamical behaviors



anticipated by the digital twin

Real Time Monitoring and Continuing Forecasting with Sparse Updates

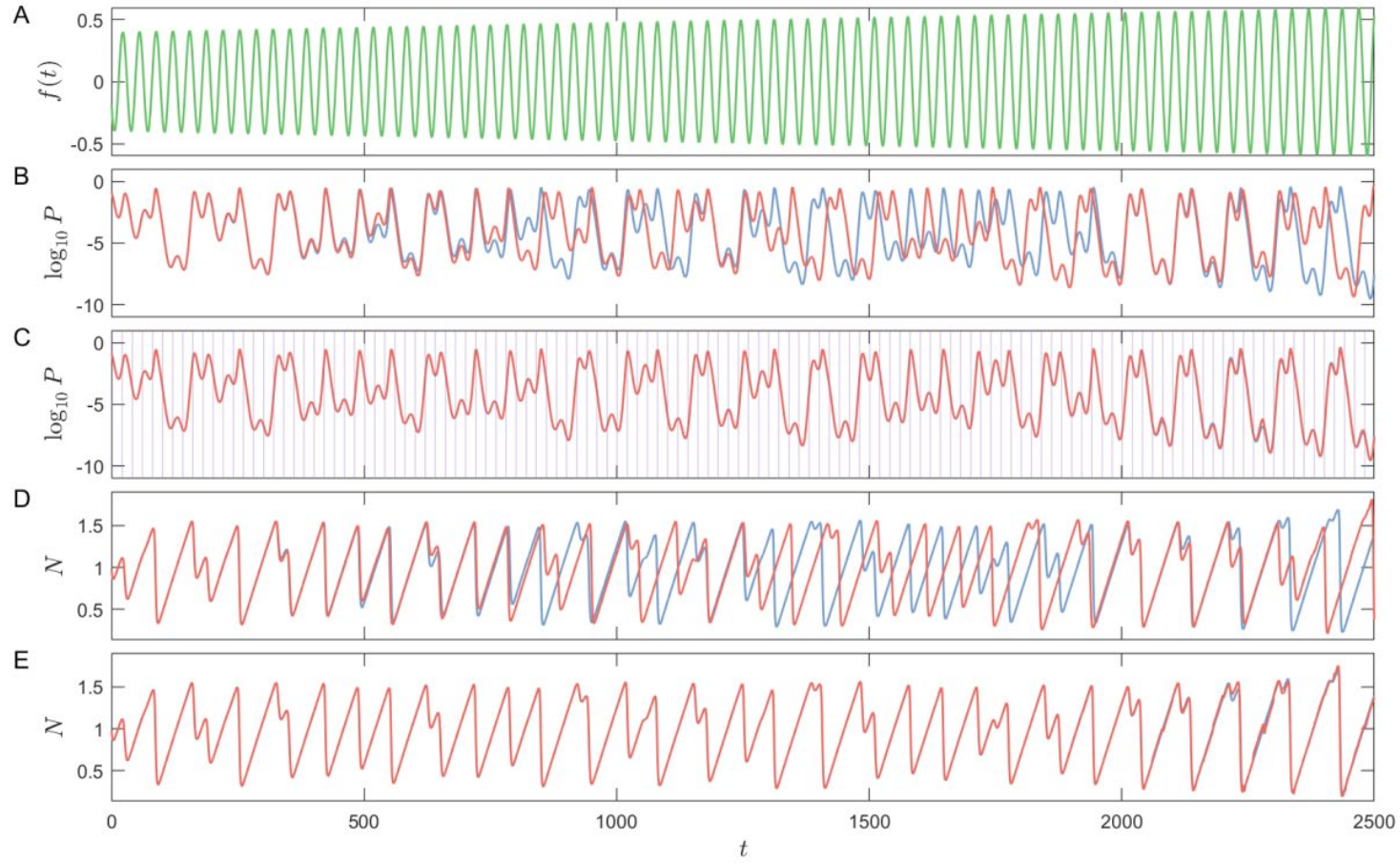
non-stationary
external driving

prediction deviates without
sparse updates

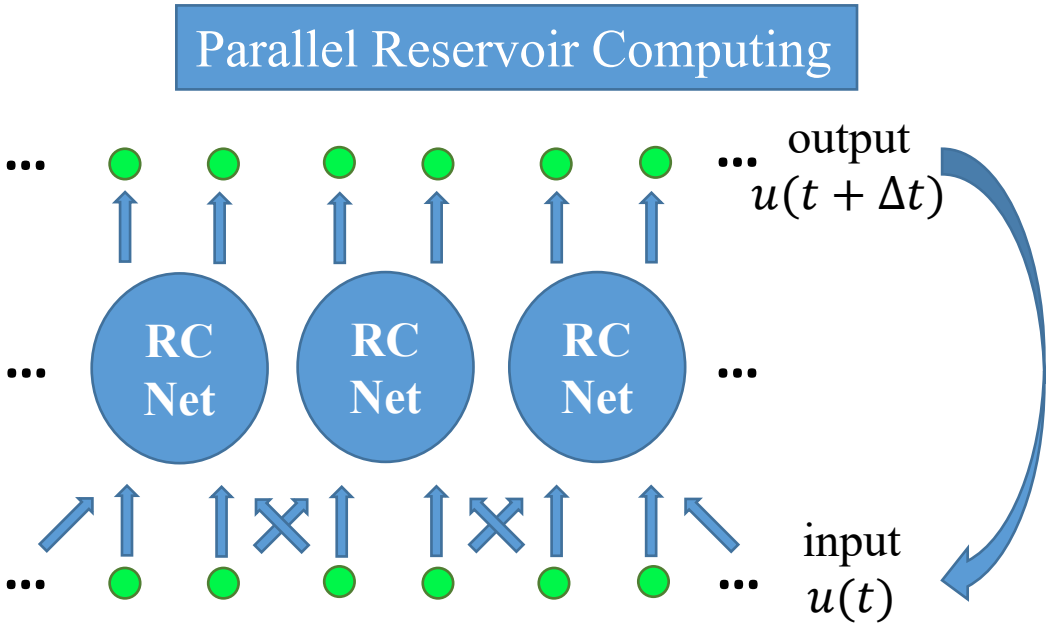
prediction with sparse updates
at the vertical stripes

prediction of a hidden variable
deviates without sparse updates

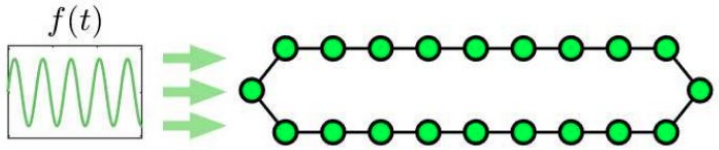
prediction of a hidden variable
with sparse updates

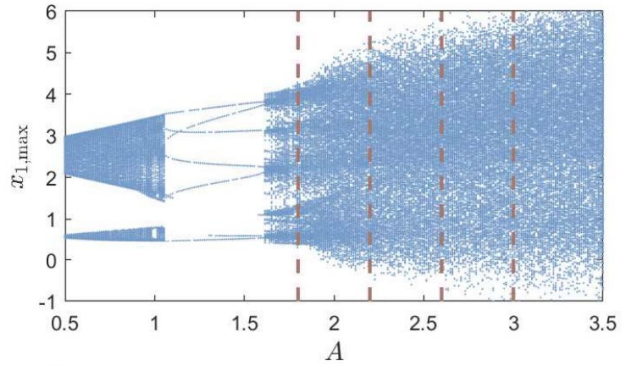


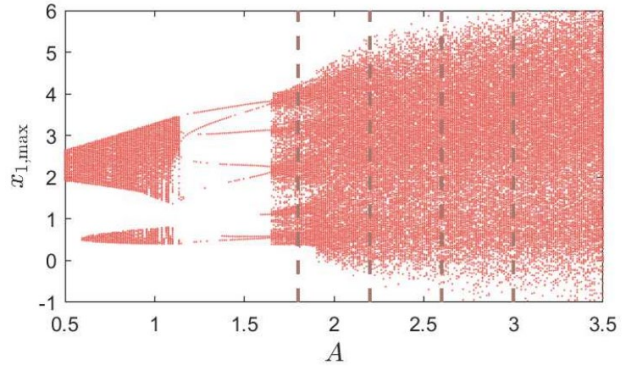
Parallel Architecture for High-Dimensional Systems



high-dimensional Lorenz-96 system with 20 oscillators in a ring structure







Product

Digital twins of nonlinear dynamical systems

Ling-Wei Kong,[1] Yang Weng,[1] Bryan Glaz,[2] Mulugeta Haile,[2] and Ying-Cheng Lai[1,3,*]

[1] *School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, Arizona 85287, USA*

[2] *Vehicle Technology Directorate, CCDC Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD 20783-1138, USA*

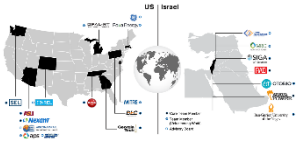
[3] *Department of Physics, Arizona State University, Tempe, Arizona 85287, USA*

(Dated: July 18, 2022)

We articulate the design imperatives for machine-learning based digital twins for nonlinear dynamical systems subject to external driving, which can be used to monitor the "health" of the target system and anticipate its future collapse. We demonstrate that, with single or parallel reservoir computing configurations, the digital twins are capable of challenging forecasting and monitoring tasks. Employing prototypical systems from climate, optics and ecology, we show that the digital twins can extrapolate the dynamics of the target system to certain parameter regimes never experienced before, make continual forecasting/monitoring with sparse real-time updates under nonstationary external driving, infer hidden variables and accurately predict their dynamical evolution, adapt to different forms of external driving, and extrapolate the global bifurcation behaviors to systems of some different sizes. These features make our digital twins appealing in significant applications such as monitoring the health of critical systems and forecasting their potential collapse induced by environmental changes.

Under review by *Nature Communications*

Next



- Study applications to realistic electrical power systems
- Work with Nexant to incorporate the principle and methodologies of digital twins for AI-based intrusion detection into the existing industrial Operational Technology and Industrial Control Systems management software tools.