# Cognitive Cyber-Physical Systems:
# Cognitive Neuroscience, Machine Learning, and Control

## American Control Conference

Pramod P. Khargonekar

Department of Electrical Engineering and Computer Science
University of California, Irvine

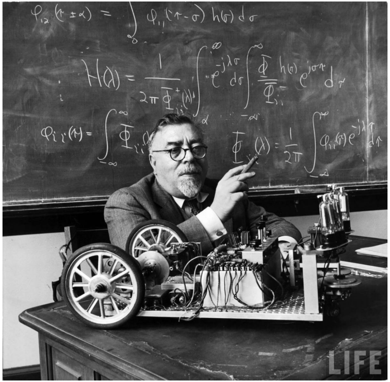
5 July 2020

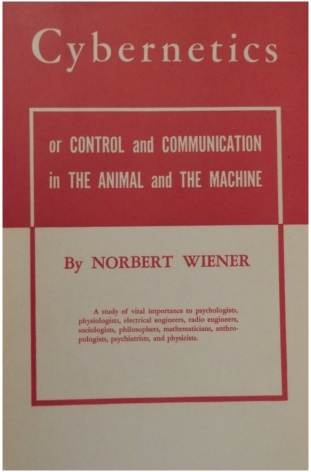
This presentation contains numerous hyperlinks (in blue) as pointers for further study and exploration.

# Outline


1. Context and Vision
2. Cognitive Cyber-Physical Systems
3. Technical Directions
4. Our Recent Work

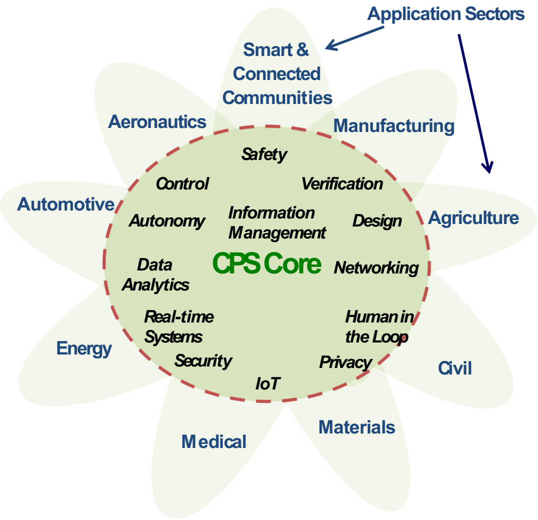
# Wiener, Cybernetics, and Macy Conferences




How would the pioneers of cybernetics and AI envision the future of CPS?

# Cyber-Physical Systems




## Application Domains

### Transportation

- Faster and safer vehicles (airplanes, cars, etc)
- Improved use of airspace and roadways
- Energy efficiency
- Manned and un-manned

### Energy and Industrial Automation

- Homes and offices that are more energy efficient and cheaper to operate
- Distributed micro-generation for the grid

### Healthcare and Biomedical

- Increased use of effective in-home care
- More capable devices for diagnosis
- New internal and external prosthetics

### Critical Infrastructure

- More reliable power grid
- Highways that allow denser traffic with increased safety

Source: NSF

# Smart-X: Conceptual View

Sensors

Communications

Internet-of-things

Automation

Data analytics

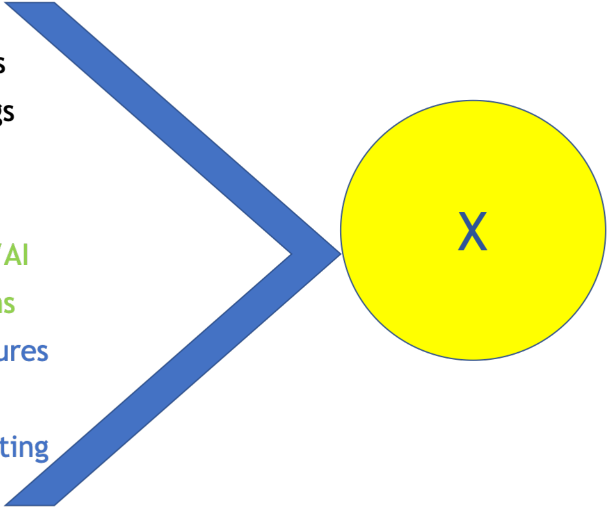
Machine learning/AI

Control/Decisions

Software Architectures

Cybersecurity

Cloud/Edge Computing



# Aspirational and Emerging Applications: Examples

- Smart-X
  1. Smart manufacturing
  2. Smart grid
  3. Smart transportation
  4. Smart cities
  5. Smart health
- Autonomous systems
  1. Unmanned air vehicles
  2. Self-driving cars
  3. Autonomous robots

Human individual and group behavior are central in many of these applications:

*Smart Cyber-Physical-Human Systems* (CPHS).

## Cognitive Cyber-Physical Systems

# Marr's 3 Levels of Analysis and Cognitive Science

Goal/Function (Computational)

Algorithm and Architecture

Implementation

Marr's 3 Levels of Analysis and Cognitive Science, Peebles and Cooper (2015)

# Cognition - Definitions and Characteristics

- "All processes by which the sensory input is transformed, reduced, elaborated, stored, recovered, and used." — Neisser, Cognitive Psychology, 1967.
- Important role of in-built capacity in the brain from genetics and evolution, e. g., symmetry, intuitive physics.
- Key Cognitive Functions
  1. Perception
  2. Attention
  3. Memory
  4. Reasoning
  5. Problem solving
  6. Knowledge representation

Cognitive Psychology, Neisser (1967)

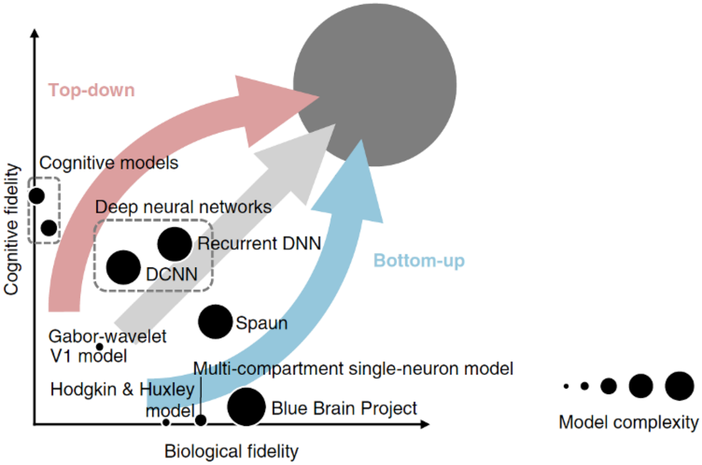
Mind as Machine: A History of Cognitive Science, Boden (2006)

# Cognitive CPS - Key Principles

- Definition: CPS that have *cognitive functions and capabilities*.
- CPS can be explicitly designed and/or can learn to possess cognitive functions.
- Need for specific cognitive functions and capabilities will depend on the problem.
- Cognitive CPS's may learn from each other, from humans, and also form collaborative networks.
- Hypothesis: Cognitive CPS will be better able to augment humans and lead to human flourishing.

**Cognitive CPS concept offers the most expansive and ambitious program for integrating ML/AI with CPHS for realizing Smart-X Systems.**

# Cognitive Models and Biological Fidelity




Cognitive Computational Neuroscience, Kriegeskorte and Douglas (2018)

# Symbolic vs. Neural Connectionist Approaches

- Historical and ongoing debate on the nature of human cognition and the structure of the brain.
- Key topic in cognitive science: neuroscience, ML/AI, psychology, linguistics.
- Three major components:
  - Computational logic systems
  - Connectionist neural network models
  - Models and tools for uncertainty
- Pragmatic approach: combine connectionist, logic and probabilistic approaches to achieve desired system goals and objectives.

Neural-Symbolic Learning and Reasoning: A Survey and Interpretation, Besold et al. (2017)

# Cognitive Models

- Production systems (Newell and Simon):
  1. If-then rules, logic, symbols
  2. Goals and subgoals, conflict resolution mechanisms
  3. Example: ACT-R, SOAR
- Reinforcement learning based models
  1. Actions, states, rewards
  2. Perception and motor modules
  3. Value and policy based approaches
  4. Three modes: Model-free, model-based, and episodic
  5. Brain combines all three of these modes but it is not known how this is done.
- Bayesian probabilistic models

# Free Energy Principle

- A most ambitious principle for brain function due to K. Friston
- Brain seeks to minimize surprise
- Bayesian brain hypothesis: brain has an internal model that allows for computation of state estimate from sensory observations using Bayes rule
- Agent chooses action policy to maximize "information gain" (KL divergence or relative entropy)
- Free energy principle: minimize expected free energy under future observations and future states
- Connections to statistical mechanics, predictive coding, risk sensitive control, . . .

The free-energy principle: a unified brain theory?, Friston (2010)

# Perception in ML

- Deep learning is revolutionizing perception
- Compositionality is built-in
- Examples of very impressive progress in:
  - Computer vision
  - Speech recognition and processing
  - Language translation
- Architectures:
  - Convolutional neural networks
  - Long Short Term Memory (LSTM) recurrent neural networks

# Perception in CPS

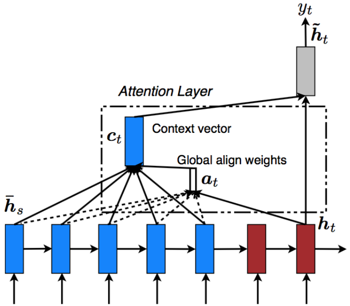
- CPS with multiple, distributed sources of sensed information
- Immediately possible to leverage DL advances
- Prior knowledge plays a very large role in cognitive theories of perception
- Neural network techniques could be combined with relational prior knowledge for improved context awareness in sensor rich CPS
- Potential tools and techniques for relational priors:
    1. Neural networks with symbolic front ends with priors to learn the symbolic front end
    2. Graph networks

# Computational Models of Attention

- Vision (human, robot, driving) has been a major focus for modeling of attention
- Feature integration theory, guided search model, CODE theory of visual attention, signal detection theory, ...
- Computational models:
  1. Itti's model: color, intensity, orientation
  2. Bayesian models of attention
  3. Decision theoretic models
  4. Information theoretic models
  5. Graphical models
  6. Spectrum analysis models

# Attention in ML

- Attention is the key to focusing on the most relevant information from multiple distributed sources of information
- Examples:
  - Recurrent Models of Visual Attention, Mnih et al. (2014)
  - Effective Approaches to Attention-based Neural Machine Translation, Luong et al. (2015)
  - Show, Attend and Tell: Neural Image Caption Generation with Visual Attention, Xu et al. (2015)
  - Self-attention Generative Adversarial Networks (GANs), Zhang et al (2019)




Attention based Machine Translator

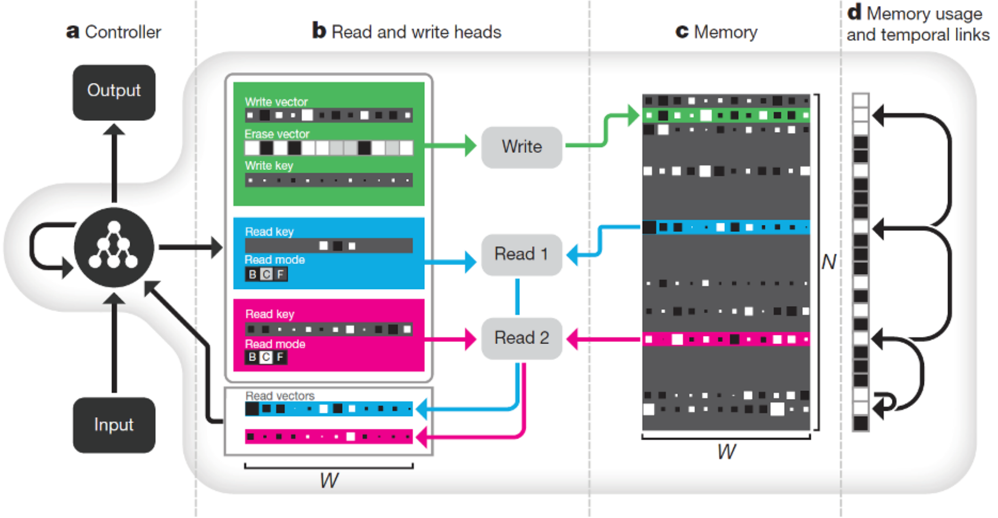
# Possible Routes to Attention in CPS

- Two levels of attention:
  - First level - selection and focus on a particular task
  - Second level - top-down search for relevant information
- Attention for detecting changing conditions and contexts.
- Attention for fault detection and/or resilience.
- Attention models that are hierarchical and programmable will be required for CPS
- Examples of programmable attention:
  1. Self-attention models of deep learning
  2. Non-local neural networks for image recognition
  3. Attentive meta learners

# Memory

- Memory is central to intelligent behavior.
- Multiple memory mechanisms in human cognition:
  - short-term
  - long-term
  - episodic (content-addressable)
  - semantic
- LSTM - excellent example of use of memory in machine learning
- Experience replay - a key innovation in Deep RL breakthroughs
- Differentiable neural computer by Graves et al. (2016)
- Sparse distributed representations. Examples: hierarchical temporal memory, sparsey

# Differentiable Neural Computer




Hybrid computing using a neural network with dynamic external memory, Graves et al. (2016)

# Memory, Attention, and Composition Cell Architecture

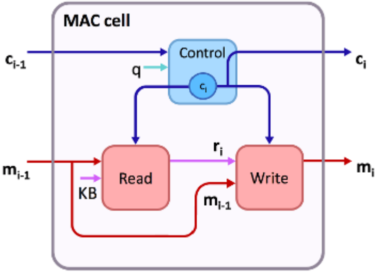



**Figure 3: The MAC cell architecture.** The MAC recurrent cell consists of a control unit, read unit, and write unit, that operate over dual ***control*** and ***memory*** hidden states. The **control unit** successively attends to different parts of the task description (question), updating the control state to represent at each timestep the reasoning operation the cell intends to perform. The **read unit** extracts information out of a knowledge base (here, image), guided by the control state. The **write unit** integrates the retrieved information into the memory state, yielding the new intermediate result that follows from applying the current reasoning operation.

Hudson and Manning (2018)

# Example of Memory in CPS: Episodic Control

- Episodic control - re-enact successful episodes from memory storage.
- Episodic control has potential relevance to “small data” learning and control.
- Example: Model-free episodic control, Blundell et al. (2016)
- Model-free episodic control – recorded experiences are used as value function estimators.
- Neural episodic control – combining deep learning model and lookup tables of action values.
- Hierarchical episodic control – episodes as options.

# Selected Methodological Challenges

- There are numerous major challenges:
- Approaches for combining model-based and model-free techniques.
- Approaches to combine hierarchical and distributed architectures and algorithms.
- Reducing the need for large amounts of data: few-shot learning, one-shot learning
- Bringing meta learning paradigm for achieving autonomy: “learning to learn”.

# Combining Model-based and Model-free Approaches

- Model free ML based approaches for sensing, perception, memory and model-based for planning, safety and closing the loop
- Model predictive control and reinforcement learning – compute action sequence based on the model via MPC (model based), update the model via reinforcement learning and supervised learning
- Guided policy search – robust local policies are derived from local models; local policies used to guide a global policy

# Hierarchical Control

- Hierarchical structures appropriate and necessary for control and management of Smart-X
- Optimal behavioral hierarchy, Solway et al. (2014)
- Hierarchical control for sparse reward settings: meta controller sets the intermediate goal/sub-tasks and a lower level controller achieves the goal
  Example: Hierarchical DQN
- Hierarchical control provides scalable methods for large state-action spaces.
  Examples:
  - Options framework – temporally extended sequence of actions to simplify the learning process
  - Feudal RL – Higher level task is divided into a hierarchy of tasks
  - MAXQ framework: extension of the Q learning framework for the hierarchical setting

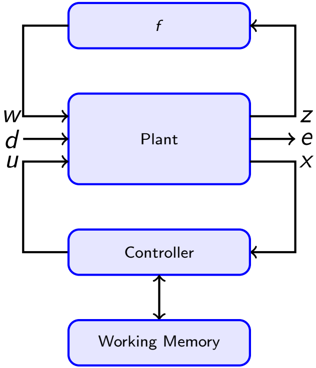
# Meta Learning Paradigm

- Meta Learning as a paradigm for dealing with new environments by “learning to learn” approaches
- Learning from task properties, *transfer learning* from prior models, . . .
- Meta learning approaches for perception
  - Optimization based approaches – the optimizer is trained for learning effectively from fewer examples in a novel task
  - Metric based few shot learning – learn a distance metric that is effective for classification from fewer examples. Examples: Siamese Neural Networks
  - Attention based meta learners. Example: hierarchy of temporal convolutions interspersed with attention layers
- Meta learning principles and approaches should be leveraged for autonomy and control under uncertainty

# External Memory in Control including Attention

**Theme: External memory to improve learning/adaptation in control systems.**

- Plant represents the system to be controlled. $u$: control input, $x$: system state.
- Function $f$ is the uncertainty in the system model.
- Traditionally, the dynamic state of the controller constitutes the "memory".
- Idea: Controller can read from and write to the *external working memory.*
- External memory is distinct from the "state" of the feedback controller.



# Publications for More Details


1. D. Muthirayan and P. P. Khargonekar, “Working Memory Augmentation for Improved Learning in Neural Adaptive Control,” IEEE Conference on Decision and Control, pp. 2019, pp.
2. D. Muthirayan, and P. P. Khargonekar, “Memory Augmented Neural Network Adaptive Controllers: Performance and Stability”, arXiv preprint arXiv:1905.02832, 2019
3. D. Muthirayan, and P. P. Khargonekar, “Memory Augmented Neural Network Adaptive Controller for Strict Feedback Nonlinear Systems,” arXiv preprint arXiv:1906.05421, 2019
4. D. Muthirayan, S. Nivison and P. P. Khargonekar, “Improved Attention Models for Memory Augmented Neural Network Adaptive Controllers,” arXiv preprint arXiv:1910.01189, 2019, Proceedings of American Control Conference, 2020. Talk by D. Muthirayan at this conference.

Thank you!

email: pramod.khargonekar@uci.edu
website: https://faculty.sites.uci.edu/khargonekar/