Envisioning Smart CPHS that Deliver Societal Benefits

Workshop on Systems and Control for Smart Society and
Cyber-Physical & Human Systems

IEEE CDC 2019

Pramod P. Khargonekar

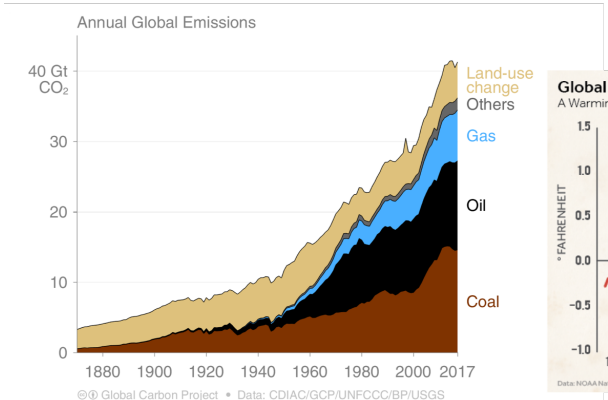
Department of Electrical Engineering and Computer Science
University of California, Irvine

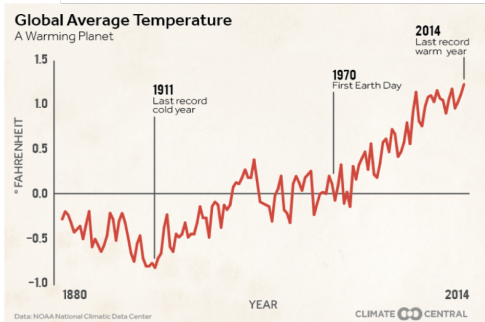
12 December 2019

Outline

Past

Fossil Energy Driving Industrial Society and Global Warming





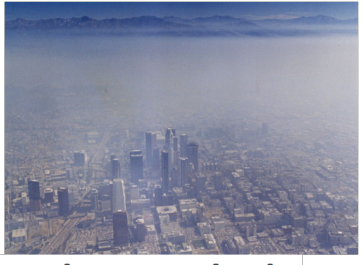
LA Transport Innovations yet Traffic Problems Getting Worse

1881

1911

1930's

1953

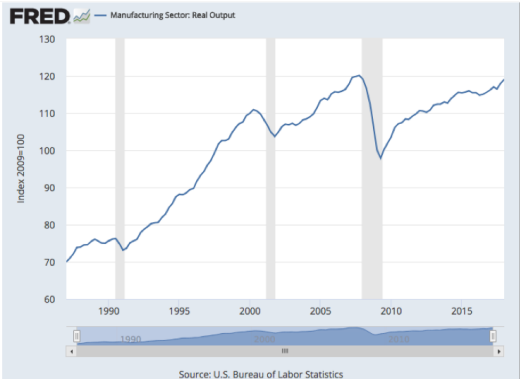


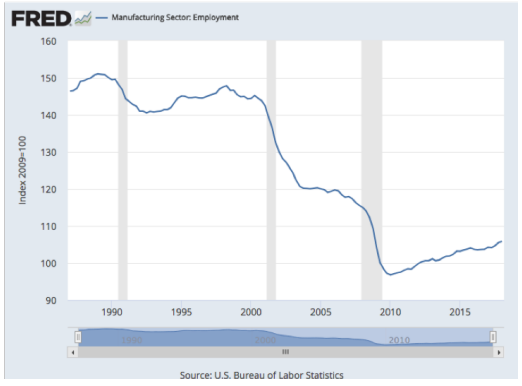
1990

The most anticipated transit projects opening in time for the 2028 LA Olympics

From the subway extension to the Westside to a people mover at LAX

US Manufacturing — Large Growth at Much Lower Employment





Automation + Globalization

Internet Revolution

"The original idea of the web was that it should be a collaborative space where you can communicate through sharing information."

Tim Berners-Lee

Technological Innovations have (UN)intended Consequences

The Internet Apologizes ...

Even those who designed our digital world are aghast at what they created. A breakdown of what went wrong — from the architects who built it.

By **Noah Kulwin**

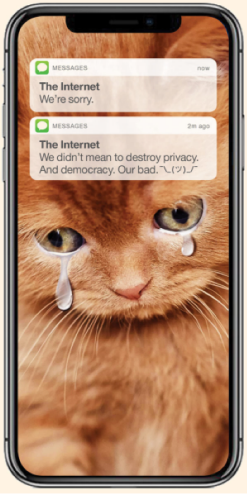
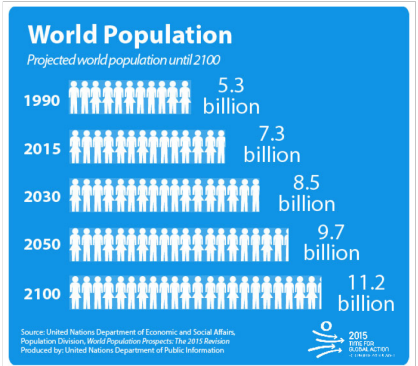


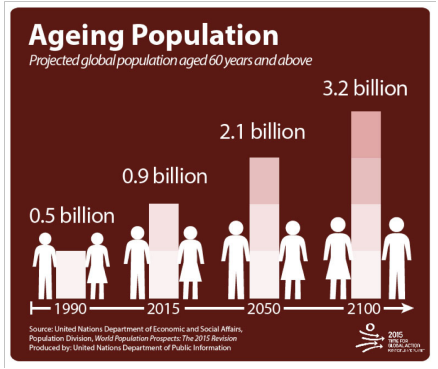
Photo-illustration by Joe Darrow

an-apology-for-the-internet-from-the-people-who-built-it

Future

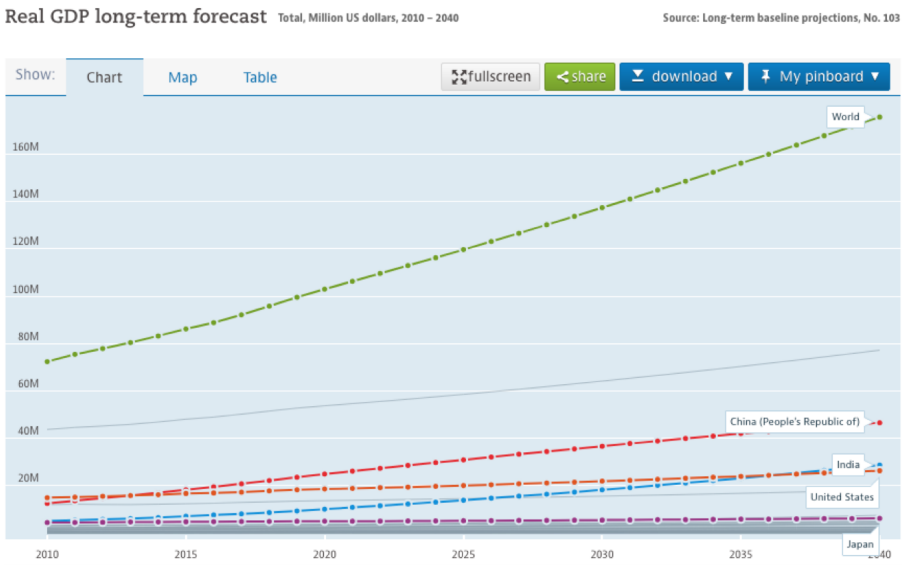
Growing and Aging Population





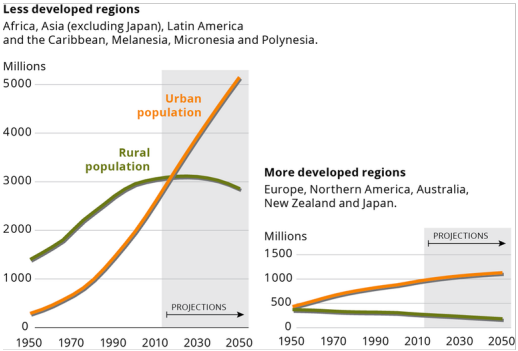
- Enormous challenges and opportunities from these demographic changes: economy, jobs, food, water, energy, infrastructure, health, wellbeing, global warming, governance, migration, ...
- Complex, interconnected, evolving, interdependent socio-economic-technological *systems*.

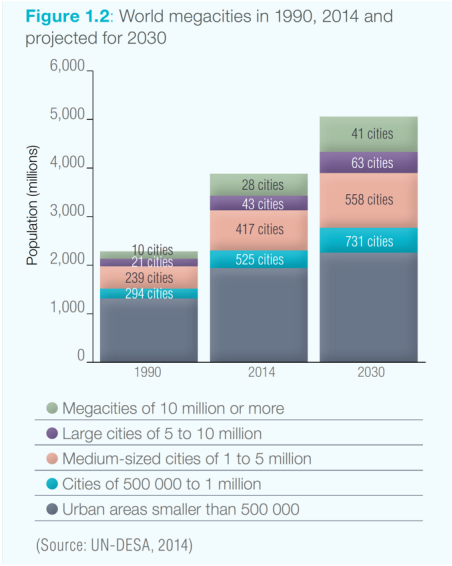
Global Economy will Double in the Next 20 Years



Source: OECD

Great Global Urbanization

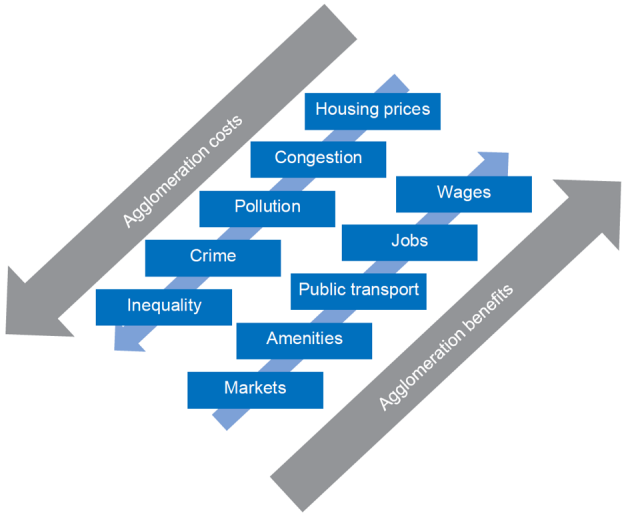




Source: European Environment Agency, UN

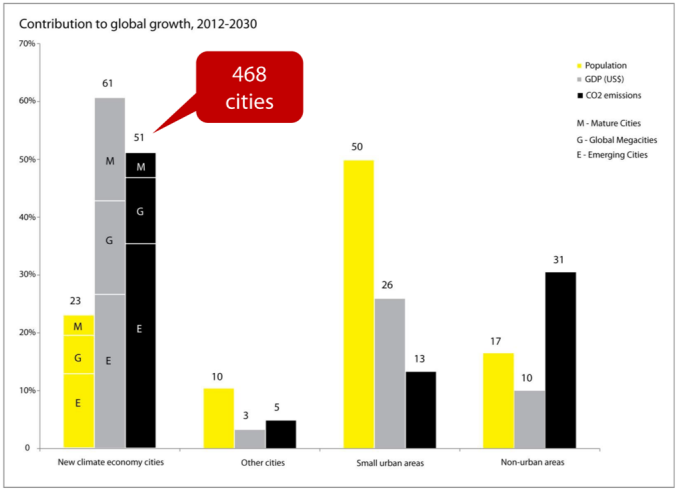
Cities have Costs and Benefits

Figure 3.1. **Large cities have benefits and costs**



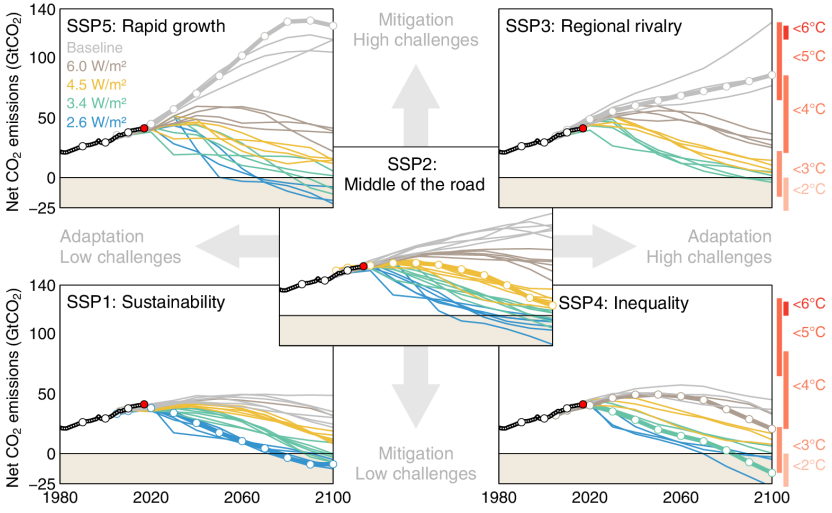
Source: OECD, The Metropolitan Century, 2015

Cities will Drive Economic Growth and CO2 Emissions



Source: Floater, Rode et al. 2014, Cities and the New Climate Economy: The Transformative Role of Global Urban Growth.

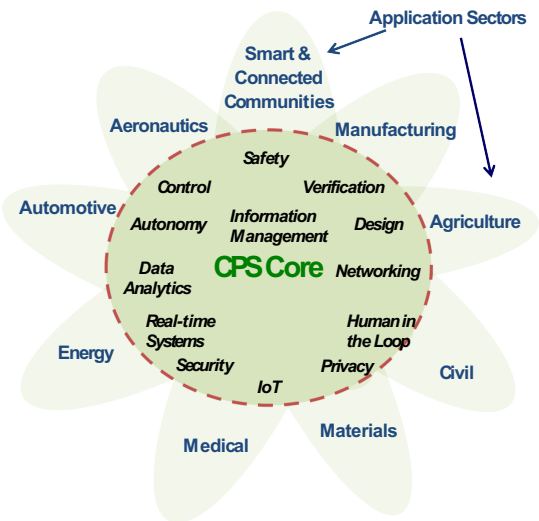
Global Warming Mitigation and Adaptation Futures



Source: Global Carbon Project

Cyber-Physical-Human Systems

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

CPS Properties

- Pervasive computation, sensing, and control
- Networked at multiple scales
- Dynamically reorganizing/reconfiguring
- High degrees of automation
- Dependable operation with potential requirements for high assurance of reliability, safety, security and usability
- With or without human interaction/supervision
- Conventional and unconventional substrates/platforms
- Range from the very small to the large to the very large

Source: NSF

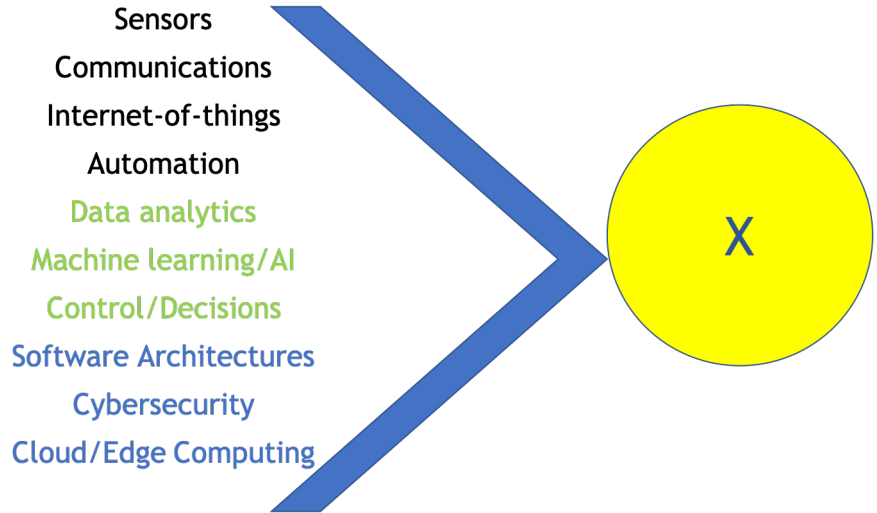
Aspirational and Emerging Applications: Examples

- 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 is central in many of these applications:

Cyber-Physical-Human Systems (CPHS).

Smart-X: Conceptual View

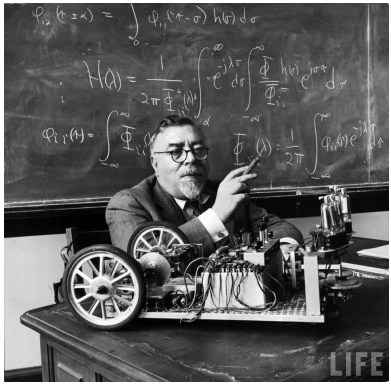


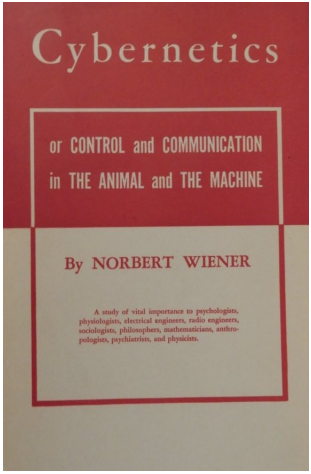
Smart-X Future

Challenge: Design, operation, management and control of large, distributed, heterogeneous, complicated, interconnected, uncertain, dynamic techno-socio-economic systems.

Vision: CPS will play a central role but will need to integrate with ML/AI and enable human flourishing.

Wiener, Cybernetics, and Macy Conferences

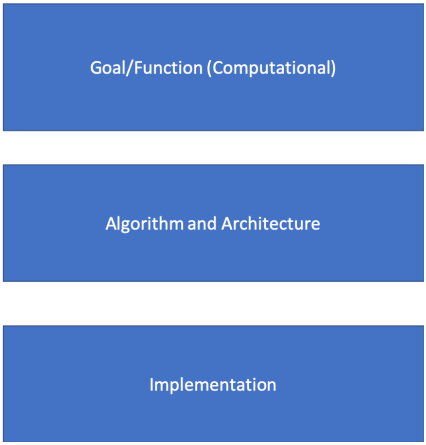




How would the pioneers of cybernetics and AI envision the future of society and Cyber-Physical-Human Systems (CPHS)?

Cognitive Cyber-Physical Systems

Marr's 3 Levels of Analysis and Cognitive Science



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, liguistics.
- 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.

Besold et al. (2017)

Computational Intelligence: Pattern Recognition or Model Building

Two fundamentally different perspectives on learning from data:

1. Statistical pattern recognition from data for prediction and control.
2. Use prior knowledge and data to build causal models to understand, predict and control.

It is possible to combine these two approaches.

Causality a critical issue.

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 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.

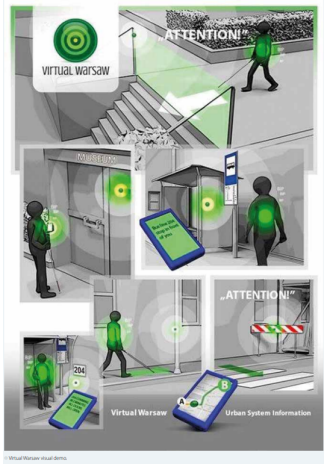
Perception in ML

- 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 priors for reasoning, e.g., NN with symbolic front ends.
  2. Graph networks, e.g., scene graphs.

Example: Virtual Warsaw — Smart City Helping Visually Impaired



"City of Warsaw launched "Virtual Warsaw", a virtual smart city based on Internet of Things (IoT) technology . . . city is deploying a network of hundreds of thousands of beacon sensors . . . to help visually impaired residents move independently about the city with assistance from their smartphones. "

EMBRACING INNOVATION IN GOVERNMENT: GLOBAL TRENDS, OECD

Attention in ML

- Attention is the key to focusing on the most relevant information from multiple distributed sources of information.
- Neurocomputational models to show that attention is important in cognition.
- 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)
  - Graph Attention Networks, Velickovic et al. (2017)

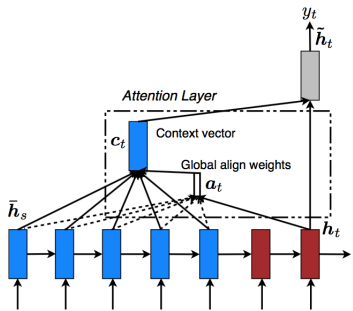


Figure: Attention based Machine Translator

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.
  4. Self-attention Generative Adversarial Networks (GANs)

Memory

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

Example Theme for Memory in CPS: Episodic Control

- Episodic control - re-enact successful episodes from memory storage and avoid unsuccessful episodes.
- 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.

Problem Solving and CPS

- Problem solving is key to enable CPS to make the optimal decisions.
- Reinforcement learning ideas and techniques are relevant in the context of goal oriented tasks.
- RL algorithms that are efficient and scalable will be necessary.
- Safety is critical for CPS.
- Potential approaches:
  1. Model based RL.
  2. Safe RL algorithms.
  3. Hierarchical RL.

Knowledge Representation

- Knowledge representation plays a role in CPS, e.g., smart manufacturing
- Knowledge representation can be of varied types: concepts, spatial and temporal relations, logic, rules, procedures.
- Traditional approaches, e.g., expert systems, had limited successes.
- Learning knowledge graphs from data and priors.
- Transfer learning using knowledge graphs.
- Connectionist models for dense distributed representations.
- Compositionality of knowledge representation.

Selected Methodological 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.
- Leveraging meta learning paradigm: “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 for control and management of Smart-X.
- 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
  - Memory based meta learners – LSTMs, DNCs
  - Attention based meta learners. Example: hierarchy of temporal convolutions interspersed with attention layers
- Meta learning principles and approaches can be leveraged for autonomy and control under uncertainty.

Example: Enabling Resilience in Smart Grids

- Three phases: pre-event, during event, and post-event
- Use of multi-sensory perception pipelines for reliable multi-time scale decisions
- Episodic control and decision making to learn from past experiences.
- Learning resilience strategies by RL on large scale simulation data.
- Meta learning methods for long-term resilience adaptation strategies.

Example: Cities are Complex Systems

"In the last fifty years our view of cities has been turned on its head. In the mid 20th century, the predominant analogy was that a city was like a machine, controlled from the top down and functioning in straightforward, ordered terms. Today we consider that cities are more like organisms."

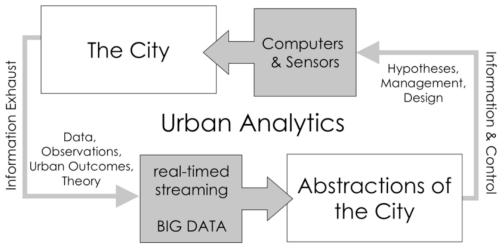


Figure 1: Understanding, Managing, Planning the Smart City

Source: M. Batty, The Age of the Smart City, 2017

Example: Novel Techniques for Urban Sensing

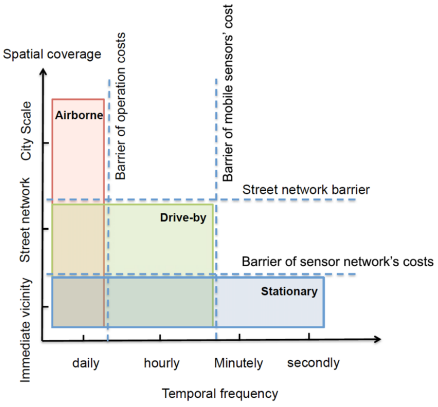


Fig. 1. Comparison of different sensing methods. Airborne sensors, such as satellites, provide good spatial coverage, but their temporal coverage is limited to the time interval when the sensors pass over the location being sensed. Conversely, stationary sensors collect data for long periods of time, but have limited spatial range. Drive-by sensing offers some advantages of both methods. By using host vehicles as "data mules," drive-by sensing offers a cheap, scalable, and sustainable way to accurately monitor cities in both space and time.

O'Keefe et al., Quantifying the sensing power of vehicle fleets, PNAS, 2019.

Example: Digital Twins to Enable Smart Cities

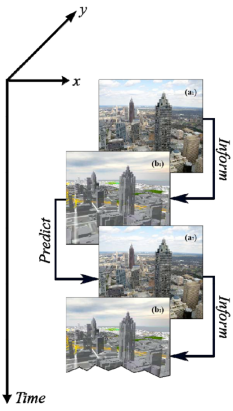


Fig. 2. Spatiotemporal Flux and Reality-Virtuality integration: Digital Twin City of Atlanta is (a) informed by the (real) city data across time and space; enabled to (b) predict future spatiotemporal states of the city. The digital twin becomes smarter in prediction over time and space as it is continuously informed by new city data.

Mohammadi and Taylor, Smart City Digital Twins, IEEE Symposium Series on Computational Intelligence (SSCI), 2017.

Example: Smart Transportation

- Greater perceptual awareness at various levels in the transportation system using distributed, connected sensors.
- Example direction for improving perception: inference on scene graph embeddings, semantic front ends, incorporation of knowledge graphs, graph networks.
- Meta learning methods for adaptation to novel circumstances.
- Use of cognitive functions in self-driving cars for better interactions with human driven cars.

Example: Smart Manufacturing

- Perception approaches for manufacturing system awareness across the supply chain.
- Transfer learning to leverage inherent parallelism in manufacturing enterprises.
- Episodic control for dealing with common disturbances.
- Cognition in digital twins for rapid adaptation and scaling of knowledge.

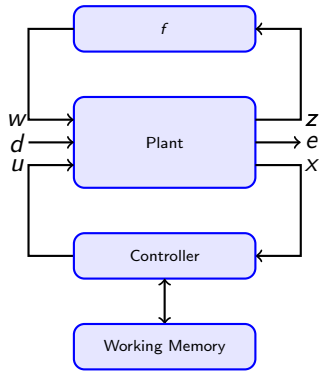
Our Recent Work

- Integration of renewable energy into electric power systems
- External memory to improve learning/adaptation in control systems.
- Social responsibility and ethics of cyber-physical-human systems.

External Memory in Control

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

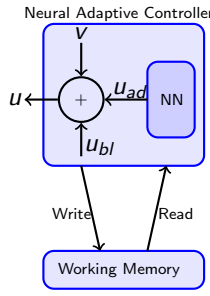
- Plant represents the system to be controlled. u: control input, x: system state.
- Function f is the uncertainty in the system model.
- Traditionally, the dynamic state of the controller constitutes the "memory".
- Idea: Controller can read from and write to the *external working memory.*



Working Memory Augmented Neural Adaptive Control

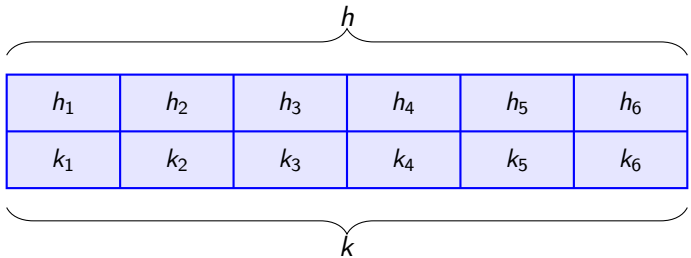
- u_{bl}: baseline control input using standard model-based (robust) control design.
- u_{ad}: control term for compensating the uncertainty f. It is the output of NN.
- v: robustness term for nullifying the higher order residual terms.
- Memory read is used to modify the output u_{ad} from NN
- Control equation:

$$u = u_{\text{bl}} + u_{\text{ad}} + v \tag{1}$$



Working Memory Structure

Working memory with six memory locations. Upper row is the matrix h of content vectors. Lower row is the matrix k of key vectors. Key k_i serves as an indentifier for content vector h_i.



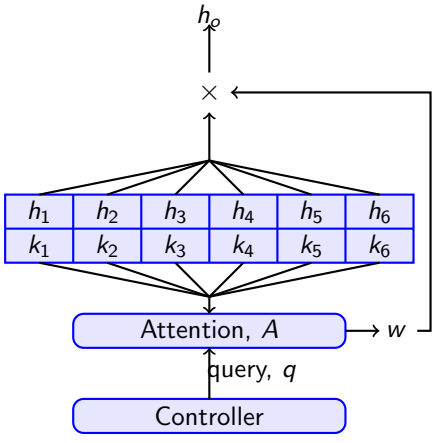
$h = [h_1, h_2, ..., h_6],\ k = [k_1, k_2, ..., k_6]$

Interface Operation: Memory Read

- A query q generated by the controller to read from memory
- Memory read equation:

$$h_o = hw = \sum_i w_i h_i \qquad (2)$$

- Vector of weights w determined by an *attention mechanism:* $w_i = A_i(q, k)$



Examples of Attention Mechanism

- Soft attention: $w = A(q, k) = \text{softmax}(q^T k)$
- Hard attention: $w_i = A_i(q, k) = \begin{cases} 1 & i = i_s \\ 0 & \text{otherwise} \end{cases}$, $i_s = \arg\max_i \|q - k_i\|_\infty$
- Attention weights are determined by how similar are the keys to the query
- Very recent work: *hard attention with attention reallocation*

Interface Operation: Memory Write

- The write vector that carries the new information is denoted by h_w
- Write operation is modeled by a differential equation with a forget term, an update term and an additional third term that is an update by the learning algorithm,

$$\dot{h}_i = -w_i h_i + c_w w_i h_w + w_i \hat{W} h_e^T \tag{3}$$

  where w_i are the same attention weights
- The factor c_w is a design parameter that controls the extent to which the write vector can update the memory.

Intuition behind the Write Operation

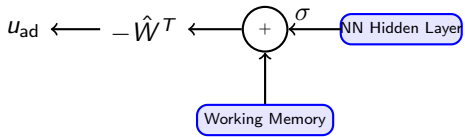
- Memory Write:

$$\dot{h}_i = -w_i h_i + c_w w_i h_w + w_i \hat{W} h_e^T \tag{4}$$

  where w_i is the output of attention, which is a measure of relevance of the write vector h_w to h_i
- Forget term erases the contents at the rate determined by the attention weights w_i
- Update term updates at the rates determined by the attention weights w_i
- Last term is technical and arises from Lyapunov stability considerations.

Modification of Control Input in Neural Adaptive Control

- Two layer NN: $\hat{W}^T\sigma(\hat{V}^T x + \hat{b}_v)$
- Memory Read output, h_o
- Memory Read h_o modifies the context for the output layer of the NN



- *Memory augmented adaptive control:*

$$u_{ad} = -\hat{W}^T\left(\sigma(\hat{V}^T x + \hat{b}_v) + h_o\right) \tag{5}$$

Memory Interface Design for Moderate Abrupt Changes

- It follows from Eq. (5) that $h_w = \sigma(.)$ (hidden layer output).
- For the setting where abrupt changes in f are not large, it is appropriate to set,

$$q = h_w(\text{new information}), k = h \tag{6}$$

- Attention mechanism – soft or hard attention
- Attention weights correspond to similarity of current hidden layer output to the memory contents

Learning Conjecture

For the proposed memory augmented NN adaptive controller, at the instant of an abrupt change (moderate), learning is accelerated through an induced learning mechanism which facilitates quick convergence to a neural network that is a good approximation of the function f after the abrupt change

Application to Flight Control

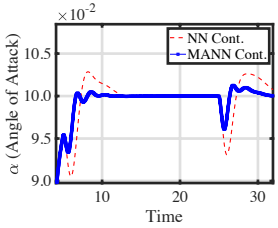


Figure: Comparison of MRAC flight controllers with and without Memory. Reference Signal (s): 0.1 deg

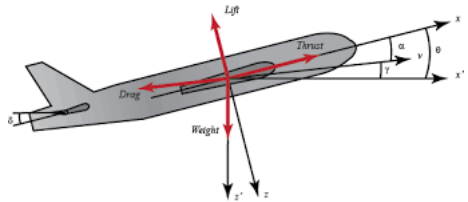


Table: Flight Controller Performance

Metric	Peak Deviation	Settling Time (1 % error)
NN cont.	0.54^o	6.61 s
MANN Cont.	0.38^o	3.45 s
Reduction	$\sim$ 30%	$\sim$ 48%

Application to Two Link Planar Robot Arm

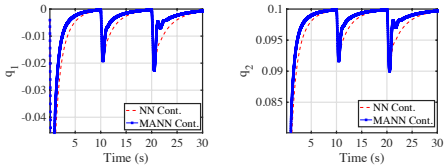


Figure: Joint angle responses for controllers with and without memory. Left: joint variable x_1, right: joint variable x_2. Reference signal, $s_1 = 0, s_2 = 0.1$

Table: Robot Arm Controller Performance, Settling Time (1 % error), First abrupt change

Joint Angle	1	2
NN cont.	17.6 s	15.2 s
MANN Cont.	16.3 s	13.7 s
Reduction	7.8%	10.4%

Table: Robot Arm Controller Performance, Settling Time (1 % error), Second abrupt change

Joint Angle	1	2
NN cont.	29.7 s	26.72 s
MANN Cont.	28.5 s	24.9 s
Reduction	4%	6.8%

Peak deviations are nearly identical

Analytical Result on Stability

Assumption

We assume that the reference signal and its derivatives (up to a certain high order) are bounded.

Theorem

Let the memory augmented controller be specified by the control law (1)*, NN update laws, memory write* (4)*, memory read* (2) *and NN output modification* (5)*. Suppose Assumption* (1) *is satisfied, and the control gains are sufficiently large, then the closed loop system is uniformly ultimately bounded.*

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, 2019, to appear.
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

Concluding Remarks: Cognitive CPS as Vision for the Future

- Cognitive CPS is a potential vision for the future of human-augmenting CPS.
- Recent advances in ML/AI offer building blocks for cognitive CPS.
- Cognitive CPS could offer new directions as ML/AI meet the physical world.
- Need to bring in (computational) cognitive science.
- Applications should drive selection of problems and development of technologies.
- Gradual development of various cognitive capabilities in cognitive CPS likely.

We are in the early stages of this exciting journey.

Thank you!

Thanks to NSF for financial support.
Thanks to D. Muthirayan for his help in preparation of this presentation.
Thanks to Fadi Kurdahi, Al-Faruque Mohammad, Zyg Pizlo, Siva Rathinam, and Nalini Venkatsubamanian for their comments.

Email: pramod.khargonekar@uci.edu
Website: https://faculty.sites.uci.edu/khargonekar/