28th Annual INCOSE international symposium

Washington, DC, USA
July 7 - 12, 2018

Adaptive Cyber-Physical-Human Systems:
Exploiting Cognitive Modeling and Machine Learning in the Control Loop

Azad M. Madni, Michael Sievers, and Carla C. Madni

Outline

- Cyber-Physical-Human Systems
- Adaptive CPHS
- Key Challenges in Adaptive CPHS
- Human Behavior Modeling in Adaptive CPHS
- Opportunities for Machine Learning
- Exemplar Adaptive CPHS
- Way Ahead

Cyber-Physical-Human Systems

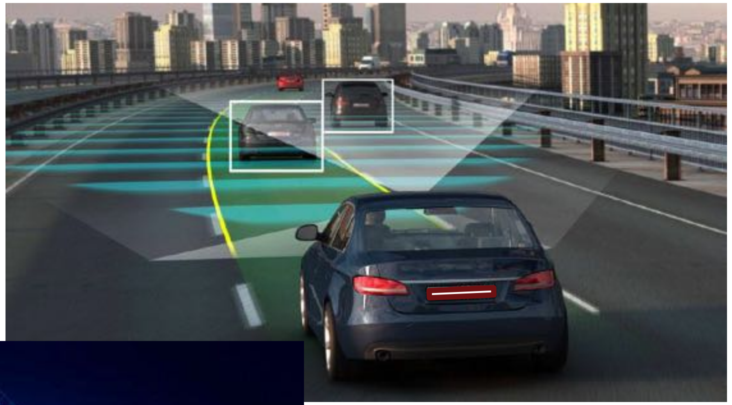
- A class of safety-critical applications in which interactions between the *physical system* and *cyber elements* that control its operation are influenced by *human agent(s),* and system objectives are achieved through purposeful interactions between the three
- A CPHS comprises:
  - **Physical model** of the system(s) to be controlled
  - **Cyber elements** (i.e., communication links and software)
  - **Human agents** who monitor CPS operation and intervene as needed
- Human intervention to redirect CPS or supply needed information as opposed to taking full control or exercising manual over-ride

CPHS Are Complex Socio-Technical Systems

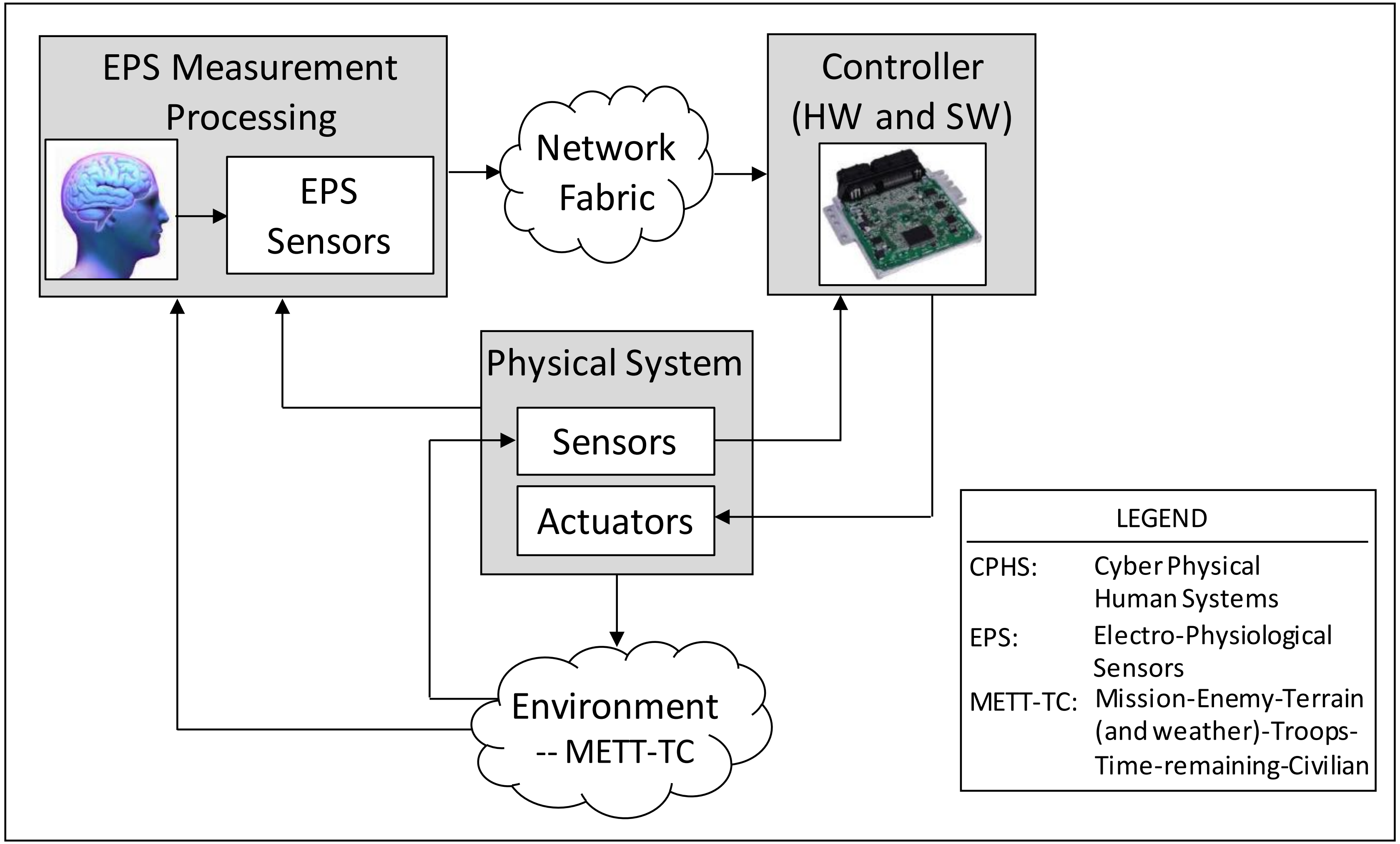
- Socio-technical
  - exist at multiple scales (CP elements, humans)
  - ability to continuously improve (learning)
  - capable of mutual adaptation (changing context)
- Complex
  - built from computational algorithms, physical components, and human agents
  - performance depends on shared context and mutual predictability especially in the face of disruptions
  - difficult to assess their long-term impact (hidden interactions, change cascades)

Exemplar CPHS

- Self-Driving Vehicles
- Smart Buildings
- Smart Manufacturing
- Medical Devices
- Unmanned Aerial Vehicles



CPHS Functional Architecture



Governance and Task Execution

- Responsibilities divided between human(s) and cyber-physical elements
- Nominal operation
  - human: high-level planning and decision making
  - CP elements: execution of detailed actions
- Contingency situation
  - safety over-rides used to avoid hazardous actions/behaviors
  - humans can intervene in CPS operation to redirect/take-over/suspend operation
  - CP elements can take over human task upon human request, or after human inactivity period exceeds a threshold and CP query of human go unanswered

Adaptive CPHS

- Humans (agents) and cyber-physical elements collaboratively adjust to unexpected or novel situations during mission execution
  - adaptive response: re-allocate tasks, restructure, re-prioritize/ re-sequence tasks, shed/discontinue task
- Respond to new missions and objectives
  - through plan adjustment, plan adaptation, re-planning, new goal
- Respond to novel situations (e.g., changes in operational environment)
  - through dynamic task re-allocation and structural re-organization
- Human roles in CPHS
  - passive sensors (e.g., social networks)
  - active performers (e.g., intrusion detection, counter-insurgency)
- Learn from experience (observations, outcomes)
  - through machine learning (supervised, unsupervised, reinforcement)

Key Challenges in Adaptive CPHS

- Inferring human intent from noisy electro-physiological sensors (EPS)
- Ensuring shared context during operation and adaptation
- Introducing strong time semantics to ensure proper synchronization sequencing of CPHS operation

Inferring Human Intent

- Electro-physiological sensors (EPS) tend to be noisy
- Noise filtering and sensor fusion partially reduce uncertainty
- Determining intent which is a key aspect of adaptive CPHS remains a challenge
- Complicating factors: emotional state, individual differences, experience, fatigue, stress

Ensuring Shared Context

- Ensure human and CP elements have a common understanding of concepts and relationships in problem domain (i.e., domain ontology such as METT-TC)
- Shared understanding of goals and plans
  - under a set of conditions, CPHS expected to behave within boundary constraints and threshold limits
  - unexpected behaviors (for any reason) are recognized and appropriate actions taken that either result in continued safe operation or cause CPHS to transition to safe operation
- **Key hypothesis:** with proper consideration of operational modes and states CPHS can be made significantly robust to errors induced by environmental uncertainty or misunderstanding of human intent

Strong Time Semantics

- Implicit in understanding modes and states is the need for strong time semantics
  - hard, semi-hard time constraints
- CPHS has to synchronize sensing, decision making and responses so that the right actions are taken at the right time to accomplish desired CPHS behaviors
  - an action taken too soon or too late can potentially prevent achievement of desired outcomes, and possibly cause an unsafe condition

Role of Human Behavior Models

- Human behavior models comprise planning and decision-making behaviors subject to cognitive limitations
- Human behavior modeling techniques range from general to specific
- Human behavior model fidelity depends on:
  - task/activity that human is engaged in
  - human interactions with cyber-physical components
  - characteristics of the operational environment
- Questions:
  - what aspects of humans should be represented for a specific adaptive CPHS?
  - is there a methodological basis for determining appropriate sparse representation of a human for a particular class of CPHS?

Examples of Human Behavior Models

- **Smart Thermostat:** uses Hidden Markov Model to model occupancy and sleep patterns of residents to save energy
  - it captures human behavior at a very high level
- **Impulsive insulin injection:** uses math models
  - for diabetes mellitus
  - very specific model determines need for insulin injection by monitoring glucose level relative to threshold level for administering insulin

Human Behavior Modeling (HBM) in Adaptive CPHS

- Purpose: reflect adaptive human behavior and interactions with CP elements
  - cognitive and emotional state: overload, fatigue, high stress, anxiety
  - infrequently arriving stimulus (events)
  - partial observability, environmental uncertainty, risk
- HBM Requirements
  - exhibit adaptability and creativity
  - understand when and how to intervene in CP processes
- Key Concepts
  - task (required knowledge/skills)
  - person (knowledge/skillset, availability, location)
  - role (qualification, training, testing, experience, location)
  - constraints (cognitive, attention, physical fatigue)

Opportunities for Machine Learning

- Multiple sources of learning
  - sensors, networks, people
- Complicating factors
  - partial observability
  - noisy sensors
  - disruptive events
- Machine learning options
  - supervised learning
  - unsupervised learning
  - reinforcement learning

Machine Learning (ML) Opportunities within Adaptive CPHS

- ML techniques can be integrated within CPH systems to:
  - learn from interacting with the human
  - learn patterns/data models from observation and analysis of operational environment
  - make decisions based on experience and evidence-derived patterns
- ML methods and tools comprise:
  - Supervised Learning:
    - requires labeled data
    - creates a data model with offline training
    - **adaptive CPHS application:** learn human's information seeking policies in different contexts
  - Unsupervised Learning:
    - creates data clusters
    - learns patterns and behaviors
    - continue learning/ training/ refining model online during execution of mission scenarios
    - **adaptive CPHS application**: learn intrusion patterns in aircraft perimeter security
  - Reinforcement Learning:
    - requires real-time interaction with environment (observation)
    - makes decisions (action) based on the existing patterns (states) and real-time environmental feedback (observation)
    - **adaptive CPHS application:** progressively learn system and environmental state based on incoming sensor reports

ML Opportunity: Learning from Human

- In learning from a human-in-the-loop, ML techniques can be employed for learning:
  - human information seeking preferences as a function of context
  - human cognitive and emotional state (e.g. alert/drowsy, stressed/unstressed, calm/agitated)
- Human behavior models should be trained offline in a controlled simulation environment using simulated/recorded data
  - applicable supervised learning techniques: artificial neural networks, perceptron, support vector machines
- Develop selective fidelity human behavior models to enhance adaptive CPH system decision making
  - e.g., Knowing human cognitive state and preference structure, the CPH system can decide to proceed to action A without requesting or awaiting a response from the human

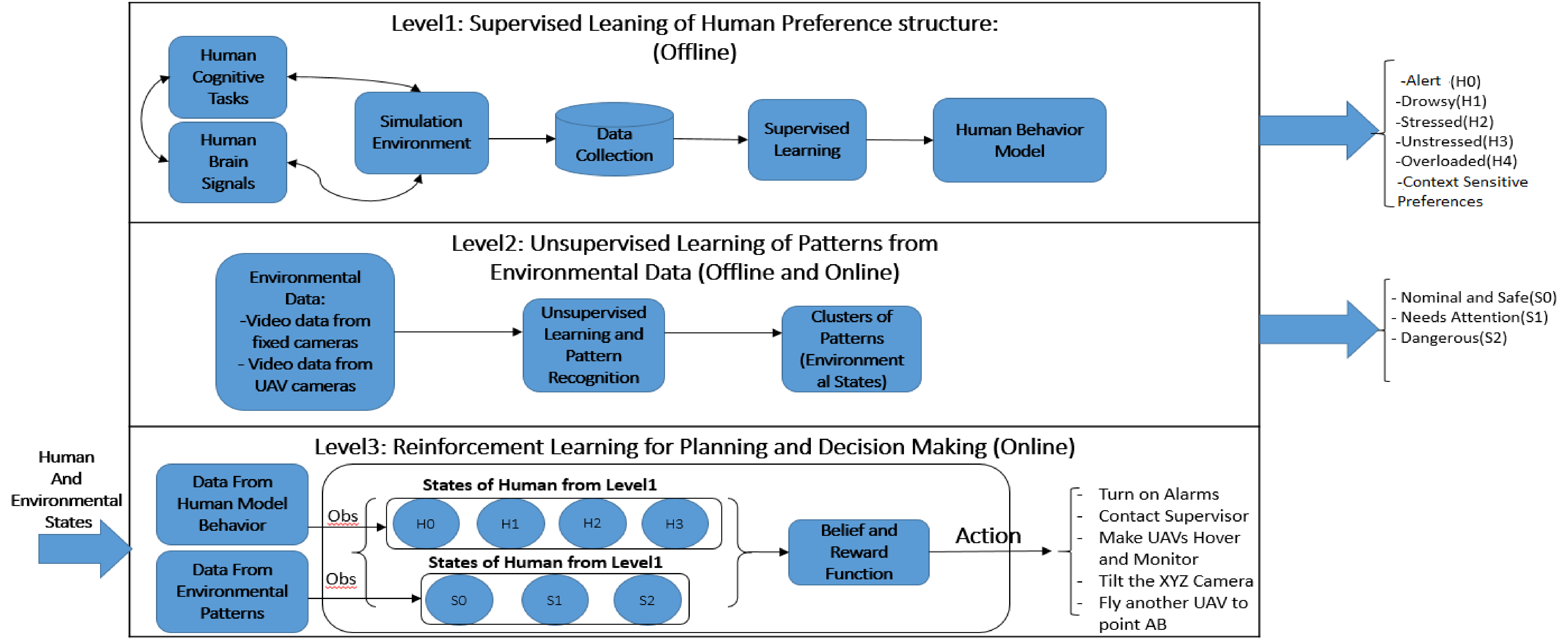
ML Opportunity: Unsupervised Learning from operational environment data stream

- Learning from sensor reports about events and incidents in the operational environment
  - exemplar sensors: any types of wireless/wired sensors, cameras, unattended ground sensors
- ML technique distinguishes between different patterns and creates clusters
- Number and shape of the clusters:
  - can be pre-defined and fixed (e.g. K-nearest neighbors algorithm)
  - can be variant and expand further if reported new patterns does not match any existing patterns or clusters
  - depends on type and variety of observed patterns (e.g. there can be only 2 clusters if patterns are used to report anomalies from normal patterns)
  - depends on the rules and boundaries that are pre-defined (e.g. data reported from a surveillance camera that is mounted on a gate can be categorized into nominal, needs attention, dangerous clusters depending on the number of people, motion patterns, and etc.)
- Unsupervised learning and pattern recognition methods for recognizing clusters and patterns in data.
- Unsupervised learning methods can use different algorithms to distinguish between patterns
  - distance-based algorithms (K-Nearest Neighbors)
  - likelihood ratio test
- Developing accurate and distinguishable clusters from patterns of data can help identify "environmental states" that can enhance CPH system decision making.

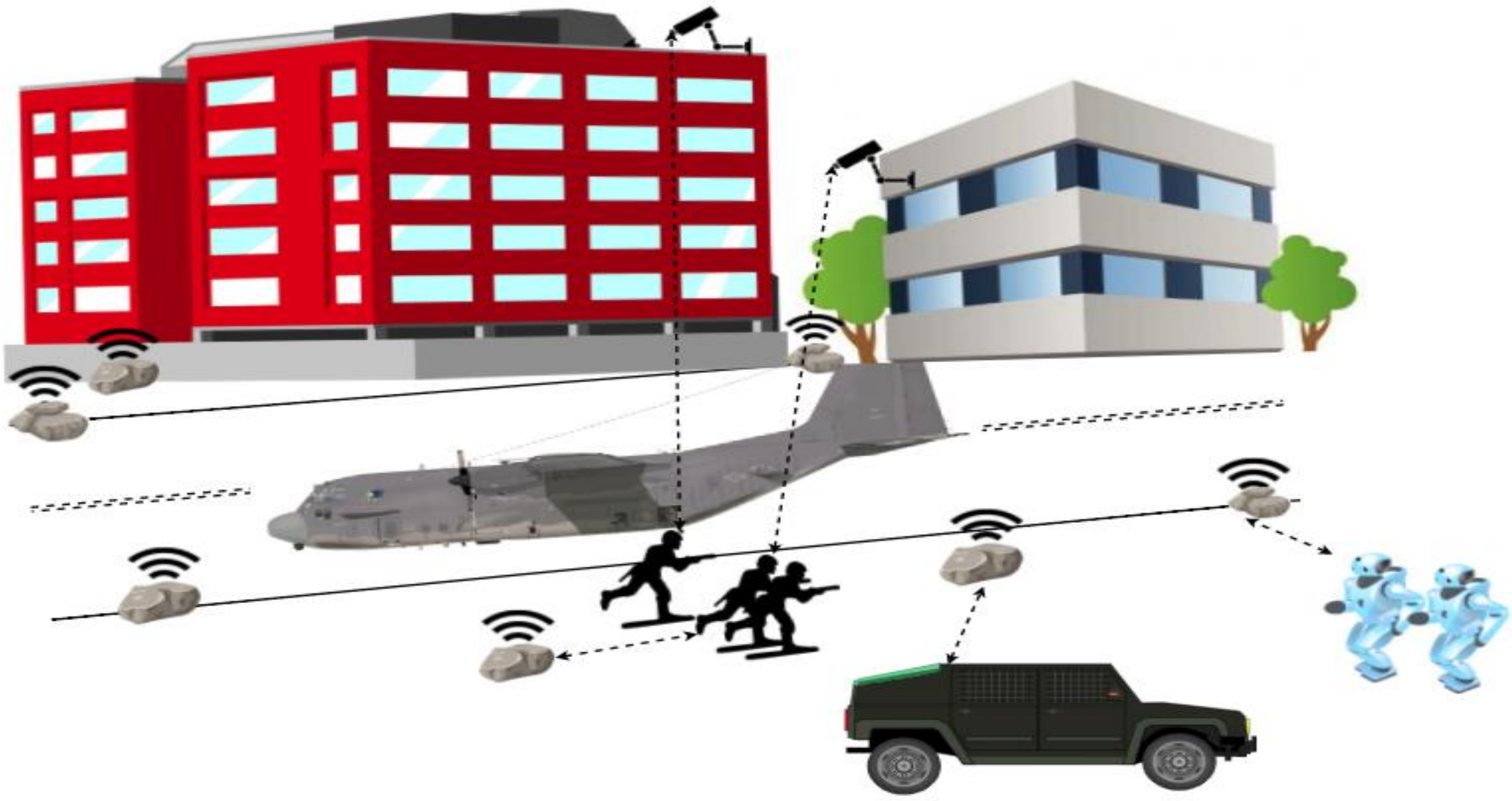
ML Opportunity: Reinforcement Learning During Planning and Decision Making

- Focus on system interaction with the environment
- Planning and decision making technique can be integrated within CPH system to:
  - offload human through intelligent automation
  - automatically generate plans and make real-time decisions based on available information (existing clusters, states, actions, and the real-time information)
- Reinforcement learning techniques can be implemented in the CPH systems for decision making based on interaction:
  - use pre-defined states (e.g. any existing clusters or states of environment and human in the loop)
  - have knowledge of the current state (either full or partial) and pre-defined actions
  - make decisions based on:
    - the indication of the state (an observation: incoming pattern)
    - maximizing the overall reward for doing the right action
- Partially Observable Markov Decision Processes (POMDPs):
  - extended version of MDPs
  - can handle partial observability of system and environment states
    - can expand existing states if unable to interpret/explain observations using existing states
  - can deal with uncertainty in environment

Exemplar ML Opportunities for Illustrative Adaptive CPH



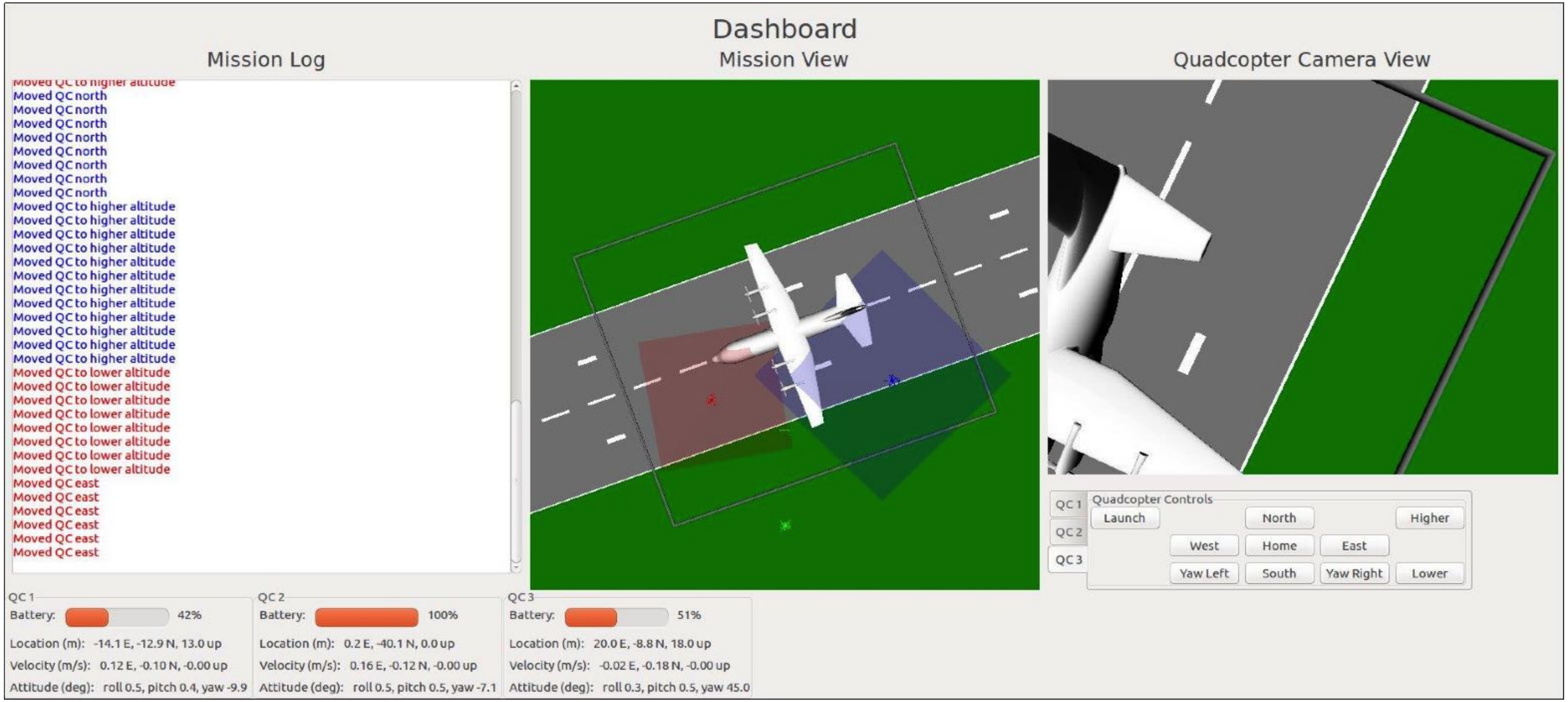
Example of Adaptive CPHS: Security of Parked Aircraft



Perimeter Coverage:
Task Reallocation Scenario

- Scenario
  - C-130 troop transport aircraft has landed on an airstrip
  - close surveillance of a perimeter about the aircraft is to be maintained
- Available automated assets
  - fixed building-mounted video cameras
  - quadcopter drones with downward facing cameras
- Goal: maintain automated video coverage of aircraft perimeter (disruptions)
  - loss of drone
  - loss of building camera
- Actions available (may be combined)
  - Reposition current flying drone
  - Launch reserve drone
- Overall states of system
  - Green (perimeter coverage maintained); Yellow (responding to disruption); Red (insufficient capability to restore perimeter coverage); in red state, CPS gives up, alerts human supervisor

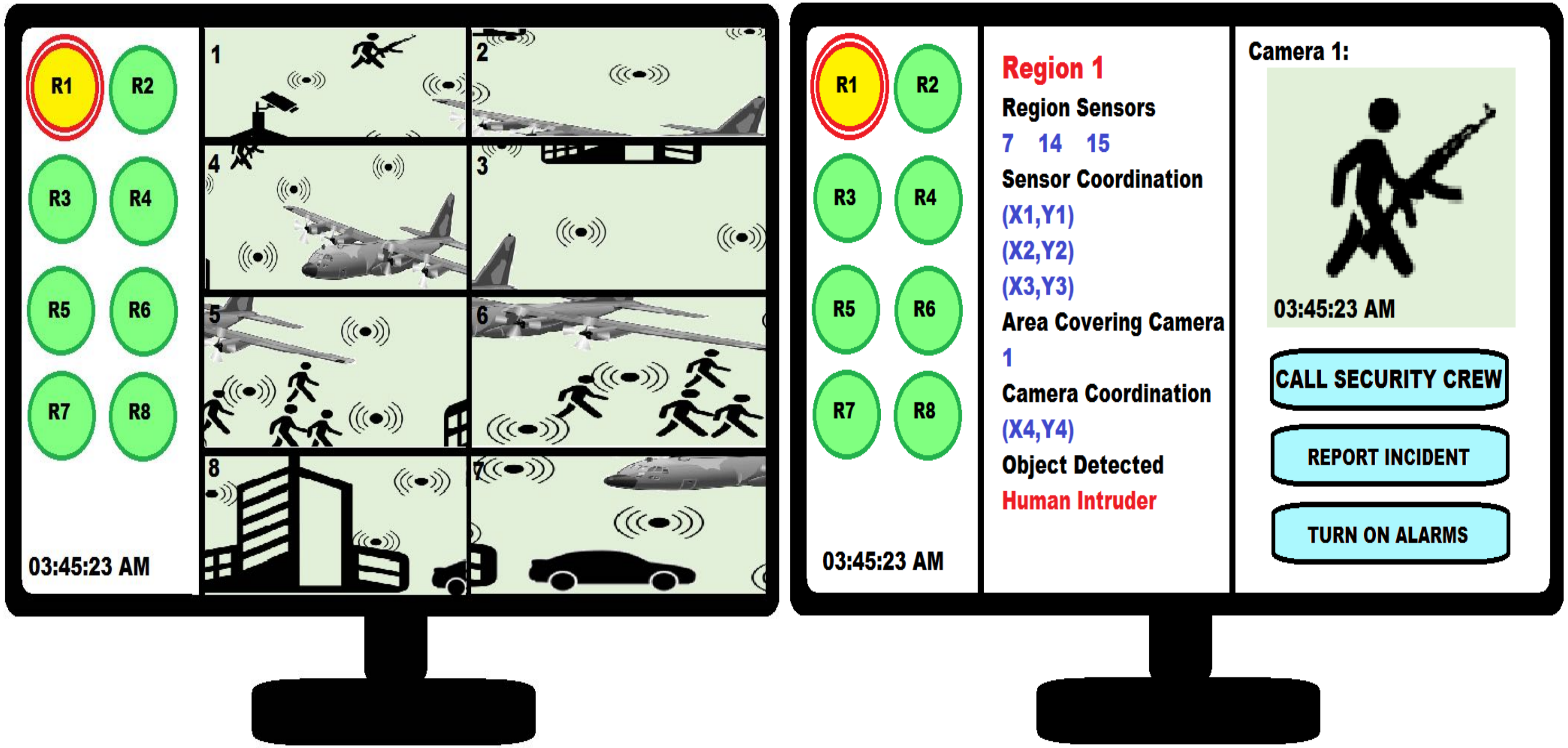
Dashboard Showing Task Reallocation



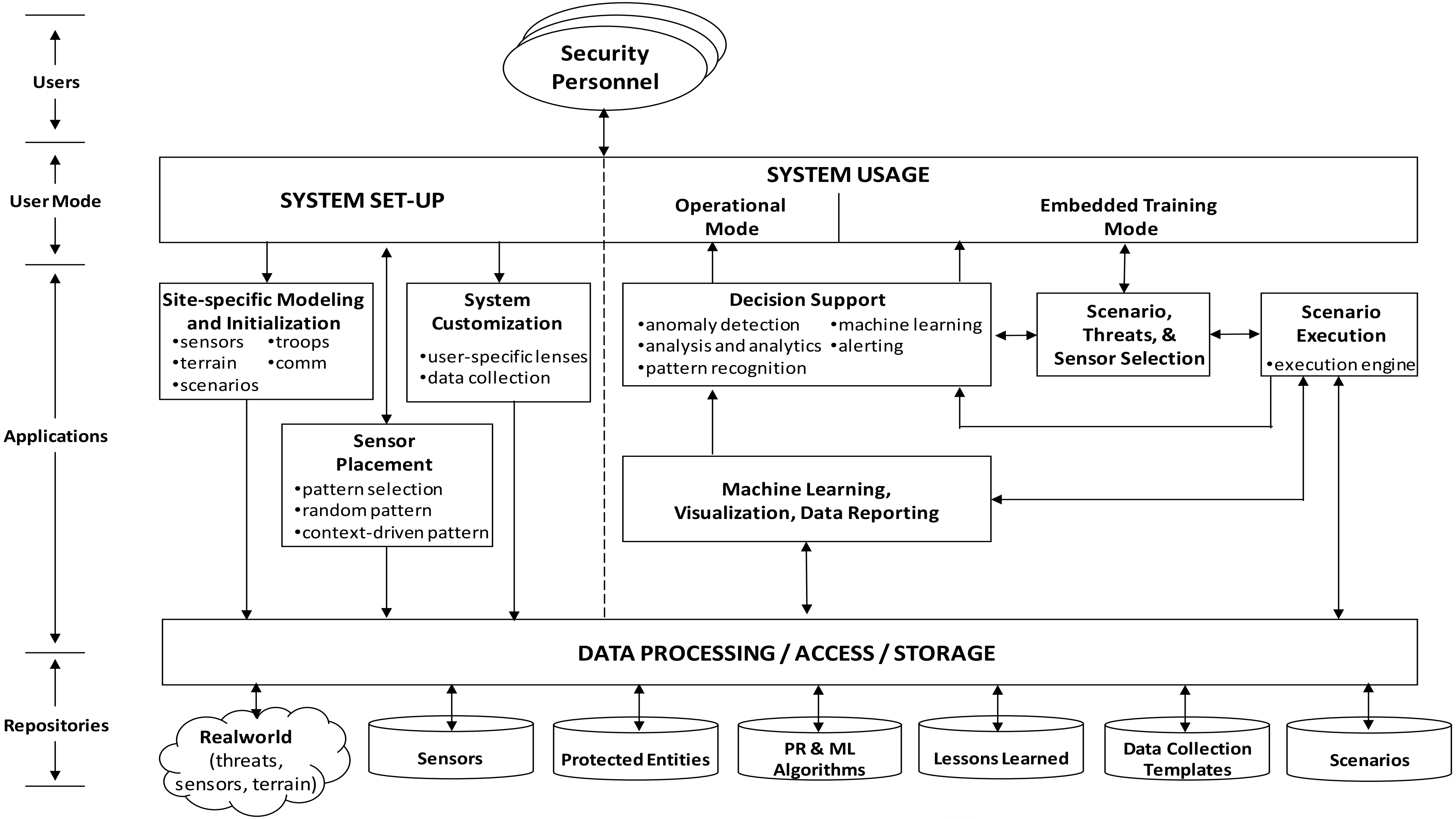
Illustrative Example : Human Roles and CPS Functions

- CPH system comprises
  - **physical:** laptop with smart dashboard software, sensors, actuators (robotic sentries); wireless connection to building mounted sensors, unattended ground sensors (UGS)
  - **cyber:** monitoring, planning, visualization, resource allocation, and ML software
  - **human:** commander in charge of maintaining aircraft security
- Human roles
  - supervisor, sensor tasking; robotic sentry tasking; human patrol tasking; intrusion monitoring; re-planning perimeter defense based on intelligence
- CPS Functions:
  - learn commander preferences and priorities in various contexts (ML);
  - learn normal traffic and intruder ingress patterns (ML), offer plans and patrol schemes;
  - generate context-sensitive visualization;
  - issue alerts upon intrusion detection; auto-reconfigure perimeter in response to changes to environment including intrusion detection (standing orders)

UI for Area Monitoring and Issuing Commands/Alerts



Layered Architecture



Key Takeaways

- CPHS are safety-critical systems in which humans can play a variety of roles
  - leads to increased complexity and vulnerability to disruptions
- Adaptive CPHS are intended to adjust their behavior when operating in uncertain, unpredictable environments prone to disruptions
- Existing system design tools that address cyber, physical, and human elements in isolation are inadequate for CPHS design
  - need to focus on interactions and change propagation
- Multiple opportunities exist for Machine Learning in adaptive CPHS
- Illustrative example shows an adaptive CPHS of interest to the military and how human behavior modeling and Machine Learning can play important roles in enhancing the performance of adaptive CPHS

References

- Madni, A.M. Mutual Adaptation in Human-Machine Teams, ISTI White Paper, January 11, 2017
- Madni, A.M. and Sievers, M. Model Based Systems Engineering: Motivation, Current Status and Research Opportunities, in *Systems Engineering*, 2018
- Munir, S., Stankovic, J.A., Liang, C.M., and Lin, S. Cyber Physical System Challenges for Human-in-the-Loop Control
- Lu, A., Sookoor, T., Srinivasan, V., Gao, G., Holben, B., Stankovic, J., Field, E., and Whitehouse, K. The smart thermostat: using occupancy sensors to save energy in homes, In *SenSys* (2010)
- Wood, A. Stankovic, J., Virone, G., Selavo, L., he, Z., Cao, Q., Doan, T., Wu, Y., Fang, L., and Stoleru, R. Context-aware Wireless Sensor Networks for Assisted Living and Residential Monitoring, IEEE Network, 22,4 (July/August 2008), 26-33.
- Shirner,G., Erdogmus, D., Chowdhury, K., and Padir, T. The future of human-in-the-loop cyber-physical systems, Computer 46, 1 (2013), 36-45.

Thank You

28th Annual INCOSE international symposium

Washington, DC, USA

July 7 - 12, 2018

www.incose.org/symp2018

Development Environment: Workflow