SYSTEMS
ENGINEERING
RESEARCH CENTER

Next Generation Adaptive Cyber Physical Human Systems

Year 1 Technical Report

September 6, 2018

Principal Investigator: Dr. Azad M. Madni, USC

Co-Investigator: Dr. Dan Erwin, USC

Research Team:

Dr. Ayesha Madni, USC

Edwin Ordoukhanian, USC

Parisa Pouya, USC

Sponsor: DASD(SE)

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) under Contract HQ0034-13-D-0004.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense nor ASD(R&E).

No Warranty.

This Stevens Institute of Technology and Systems Engineering Research Center Material is furnished on an "as-is" basis. Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF (TABLES, SEQUENCES)

ABSTRACT

Cyber-Physical-Human Systems (CPHS) are purposeful arrangements of sensors, computers, communication devices, and humans to perform tasks that achieve specific mission objectives. These systems typically allow other systems, devices, and data streams to connect/disconnect as needed during mission execution. The roles of humans in CPH systems are quite varied. In adaptive CPHS, humans collaborate with the cyber-physical elements to jointly accomplish tasks and adapt to changing contexts to accomplish mission goals. This report presents the key accomplishments of the first year of this effort.

INTRODUCTION

Cyber-Physical-Human Systems (CPHS) are complex engineered sociotechnical systems in which computers, sensing and communication devices, and humans cooperate to jointly perform missions (and tasks) over time and across space (Sowe et al., 2016). CPHS can exist at multiple scales. A purposeful combination of computational algorithms, physical components, and humans (agents), adaptive CPHS are capable of collaborating in joint task performance and adapting as needed to respond to operational contingencies and unexpected situations (Madni, 2018). Their performance depends on shared context and mutual predictability especially in the face of disruptions (Madni, 2017).

Madni (2018) defines CPHS as "*a class of safety-critical socio-technical systems in which the interactions between the physical system and cyber elements that control its operation are influenced by human agent(s). CPHS objectives are achieved through interactions between: physical system (or process) to be controlled; cyber elements (i.e., communication links and software); and human agents who monitor and influence the operation of cyber-physical elements. A key distinguishing feature of CPHS is that human (agents) intervene to redirect cyber-physical system or supply needed information, not just assume full control or exercise manual over-ride.*"

An important challenge in the design of CPHS is assuring shared context in human-CPS decision making and control. This is a challenging problem because of the nonlinear behavior of CPHS in different contexts. Existing system modeling approaches tend to employ simplistic human models (e.g., humans modeled as a disturbance to the system, human modeled as a simple transfer function) that do not take human cognitive limitations into account. However, current research at major universities is beginning to look at the development of frameworks for CPHS modeling, analysis, and verification in simulated operational environments (Madni, Madni and Sievers, 2018). For example, researchers at The Robotic Institute of CMU are conducting research in integrated human-CPS behavior with a view to developing fundamental principles and algorithms that can serve as a foundation for provably safe, robust hybrid control systems for CPHS. This group is also working on developing analytical human models that reflect cognitive abilities and limitations in interactive human control of CPS elements. Similarly, researchers at UC Berkeley are working on predictive methods on guaranteeing performance of CPHS (Robinson et al., 2016).

Adaptive CPHS are CPHS with the ability to: a) flexibly respond to unexpected or novel situations during mission execution; b) respond to new missions and objectives through plan adjustment, plan adaptation, replanning, or setting new goals; c) learn from experience (i.e., observations, feedback on outcomes) using different types of machine learning (i.e., supervised, unsupervised, and reinforcement learning); and d) incorporate humans in the role of passive sensors (e.g., social networks) and/or active performers (Madni, 2018).

Research in adaptive CPHS, is also being pursued within the U.S. Military, emergency and intensive care units, first responder systems, and smart manufacturing (Gelenbe et al., 2012). Adaptive CPHS are viewed as critical for high stress, emergency response operations (e.g., firefighting, terrorist response, intensive care, natural disaster response). In such high stress scenarios, effective collaboration between the cyber-physical elements and humans is critical to achieve desired outcomes (e.g., lives saved, damage prevented). Examples of adaptive CPHS are smart grids, smart cities, self-driving vehicle networks, smart buildings, and other instrumented, sociotechnical infrastructures that require resilience.

TECHNICAL CHALLENGES

There are multiple challenges in architecting and engineering adaptive CPHS:

Inferring Human Intent. Understanding intent is an ongoing challenge in adaptive CPHS. Electro-physiological sensors (EPS) are a key source for identifying intent but tend to be noisy. In fact, noise is inherent in any sensor-based control system. Noise filtering and sensor fusion only partially reduce uncertainty in inferring intent. Therefore, it is important to exploit contextual knowledge to increase confidence in intent determination.

Shared Contextual Knowledge. It is important to ensure human and CP elements have a common understanding of concepts and relationships in problem domain (i.e., shared domain ontology such as METT-TC). Human and CP elements need to have a shared understanding of goals, plans and system state. Under a defined set of conditions, CPHS are required to behave in a manner that complies with boundary constraints and threshold limits. Unexpected behaviors (for any reason) need to be recognized and appropriate actions taken that either result in continued safe operation, or cause CPHS to transition to safe operation. A key hypothesis is that with proper consideration of operational modes and states, CPHS can be made robust, and can withstand errors induced by environmental uncertainty or misinterpretation of human intent.

Strong Time Semantics. Need for strong time semantics is required to ensure proper synchronization and sequencing of CPHS operation. A CPHS has to synchronize sensing, decision making and responses so that the right actions are taken at the right time to accomplish desired behaviors. An action taken to soon or too late can potentially prevent achievement of desired outcomes, and possibly cause an unsafe condition.

TYPOLOGY OF ADAPTIVE CPHS

Adaptive CPHS can be conveniently classified as: systems in which humans directly control the CPS; systems in which the CPS passively monitors the human and takes appropriate actions when needed; and systems that are a combination of the two. Examples of such applications are presented in the literature (Madni et al., 1985; Munir et al., 2014).

HUMAN AND CPS ROLES IN ADAPTIVE CPH SYSTEMS

Human Control of the CPS. This type of adaptive CPH system calls for direct control of the CPS by humans, using primarily supervisory control (Sheridan, 1992). There are two cases that exist for this type. In the first case, the human is able to intervene in the CPS control algorithms to adjust set points. In the second case, the CPS accepts and carries out human commands, reports results, and awaits the next command from the human. In both cases, the human is in control of the CPS.

CPS Passively Monitors the Human and takes Appropriate Action when Needed. The CPS elements for this type of CPH system can be open-loop or closed-loop. An *example of an open-loop CPH* system is a sleep tracking device that tracks the quality of sleep (Kay et al., 2012). CPS elements in this case also monitor sound, light, temperature, and motion sensors to record environmental conditions (i.e., context) during sleep. In this example, the human is in the loop but does not directly control the system. Also, the CPS does not take any proactive action to improve sleep quality (i.e., it is an open-loop system). An *example of a closed-loop* human-in-the-loop CPS is the smart thermostat. A smart thermostat uses sensors to detect occupants in the home as well as their sleep patterns and uses the patterns to proactively turn off the HVAC system to reduce energy consumption (Lu et al., 2010).

Human Monitoring the CPS that Acts as the Controller. In this type of adaptive CPH system, control to the CPS is granted by the human (by passing the “conn”). The human can revoke control from the CPS by taking back the “conn.” The concept of passing and revoking the “conn” is a naval metaphor involving the Captain and the Officer of the Deck (OOD). In this control construct, the Captain commands and controls actuators through the OOD, or grants control to the OOD to control the actuation subsystems while maintaining the ability to rescind the “conn.” In either case, the Captain works through the OOD. In one case, the OOD is the Controller (i.e., OOD has the “conn”). In the other case, the Captain has the “conn” and the OOD accepts the captain’s command and translates them into controls for the actuation subsystems (Madni et al., 1985).

Human and CPS Roles in Adaptive CPHS. Human and machine strengths and limitations have been extensively addressed in the literature (Madni, 2010; Madni, 2011). In the light of this research, several adaptive CPHS-related questions need to be answered: 1) What roles do humans play in adaptive CPHS? 2) In what contexts do these roles come into play? 3) What is the impact of disruptions on these roles? How to architect CPHS to support the different human and CPS roles (Tables 1 and 2).

Table 1. Human Roles in CPHS and Associated Context

- **Monitor**: outside the control loop
  - monitor and interact with the environment (exclusive human awareness)
  - assess correct operation of CPS
  - intervene in the control loop if necessary
    (context: CPS requests take over; incorrect/ineffective CPS operation)

- **Supervisor**: outside the control loop
  - approve CPS decision
  - over-ride CPS decision (after taking back the “conn”)
    (context: CPS unaware of full operational context)
  - re-allocate tasks between human and CPS
    (context: erroneous CPS decision; cognitive overload/fatigue; CPS request)
- **Controller**: within the control loop
  - interact with sensors and actuators
    (context: supply information needed for control; dynamic operational environment; partial observability)
  - e.g., query sensors, (re)direct sensors/collection assets; supply missing information
  - e.g., modify actuator inputs based on information not available to the controller
- **Backup CPS**: within the control loop
  - takeover CPS control function
    (context: when CPS malfunctions, or CPS requests human takeover)

The CPS can also perform in a number of roles as shown in Table 2.

Table 2. CPS Roles in CPHS and Associated Context

- **Controller**
  - interrogate/redirect sensors
  - modify actuator inputs based on externally sensed data
  - signal handoff if CPH system headed into trouble
- **Correlator/Aggregator**
  - correlate its assessment of human state with external sensors
  - e.g., is elevated heart rate due to stress or excess caffeine?
  - collects and fuses multi-source information with proper weighting based on source reliability
- **Shared Decision Maker**
  - confirm/probe human-defined objective and retrieve known options
  - evaluate all options (including options generated by humans;) implement human selected option
- **Backup to Human**
  - be prepared to backup human by taking over specific functions/tasks under certain situations
  - e.g., inactivity period > threshold; human request; human drowsy (physiological monitoring)

Tasks performed by human or CP elements can be re-allocated based on context (inability to perform, request for help). Need ways to assess human-CPS interactions so that right (safe, correct, efficient) task allocation is achieved. Scope of tasks can change (performance, context). e.g., if human drowsy, CPS takes over, e.g., if CPS headed into trouble or signals handoff, human takes over.

CHALLENGES IN ADAPTIVE CPHS DESIGN

Existing system design methodologies and tools are inadequate for modeling and designing CPHS. CPHS are tightly coupled systems with strict timing and synchronization constraints. Existing tools lack requisite semantics and "improvement with use" capability. The specific deficiencies of existing tools are that they address cyber, physical, and human elements in isolation, not together. They lack the semantics of time and focus exclusively on subsystems, not their interactions and synchronization constraints. They tend to have implied or overly simplistic representation of human behavior. Invariably, they tend to be "build-time" approaches with no provision for learning during mission execution ("run-time").

As noted earlier, adaptive CPHS are sociotechnical systems that comprise computation, communication and control at multiple scales. With CPHS, the role of the human is multi-faceted (Madni, 2010; Madni, 2011), ranging from that of a supervisor (who can intervene in the control loop) to that of an agent (operating within the control loop). An adaptive CPHS needs to create and capitalize on the synergy between the human and CPS elements. To this end, several challenges that need to be overcome (Madni, 2010; Madni, 2011). These include:

- *Performance Degradation:* performance degradation occurs with sustained high cognitive load and/or fatigue
- *Unpredictability:* unpredictability arises from human variability in task performance
- *Human Reluctance:* humans need to be incentivized to perform as an effective team member
- *Misperception of Humans:* humans tend to be perceived as suboptimal job performances that need to be compensated for/shored up rather than as assets capable of creativity and ingenuity
- *Limitations of Humans and CPS:* dynamic function allocation can be used to circumvent limitations of both humans and CPS
- *Accuracy and Recall:* tasks that require perfect recall and computational accuracy need to be allocated to CPS
- *Search and Aggregation:* tasks that require rapid search and aggregation capabilities need to be allocated to CPS
- *Common Sense Reasoning and Novel Option Generation:* tasks that require common sense reasoning and novel option generation need to be allocated to humans
- Repetitive Tasks: repetitive tasks need to be allocated to CPS (CPS does not tire; can be augmented by additional CPS elements if overloaded)
- *Human Behavior Modeling:* aspects of human behavior that should be included in human behavior models (e.g., task demands, context; progress for cognitive limitations) are determined by model purpose and context
- *Bi-Directional Learning:* bi-directional learning is needed for mutual adaptation and effective joint performance (e.g., machine learns human preferences and intent offline; human learns machine limitations and capabilities offline; each learns the other's state

online) (e.g., human cognitive load, fatigue level, CPS availability to take over certain human tasks)

- *Shared Decision Making:* allocating decision tasks to CPS and humans to exploit their respective strengths while circumventing their respective limitations (Madni, 2014)
- *Context Recognition:* CPS needs to recognize context and determine how well (i.e., to what degree, how fast) humans can adapt in that particular context before initiating some type of adaptation
- *Role Switching:* CPS need to keep track of multiple human roles and human role switches during task performance

There are several opportunities that exist to enhance the performance of adaptive CPHS during mission execution. These include: exploring the human's ability to improvise in unfamiliar problem contexts and situations; leveraging the CPHS's ability to dynamically transfer control between the CPS and human and vice versa based on context; allowing the human to back up a malfunctioning CPS in specific contingency situations; ensuring that the human and CPS are capable of exploiting each other's strengths during interactive task performance while circumventing each other's limitations; and facilitating mutual learning during task performance. One CPS limitation is that it may not be aware of the human's awareness of the environment based on certain factors that the human discerns (i.e., exclusive human awareness). For example, in automated vehicles, the driver may perceive something that bears on decision making that the vehicle's autonomous controller might not. Similarly, changes to a goal or tasking that the human becomes aware of (e.g., radio message to the human) that requires the human to change goals or performance parameters. In this case, the CPS is not aware of this change unless the human communicates this to the CPS to re-establish shared context. Thus, when human interaction with the environment results in knowledge that the CPS is unaware of, then the human has a choice: either communicate that knowledge to the CPS so the CPS is a candidate to perform tasks that require that knowledge or make tasks requiring that knowledge exclusively human performed tasks.

A key challenge outside the scope of this effort is the vulnerability of the adaptive CPHS to cyber-attacks. As the interactions between the physical, cyber and human elements increases, the physical system becomes increasingly more susceptible to security vulnerabilities in the cyber system. Security of cyber-physical systems is a relatively nascent area. Traditional secure communication solutions are not designed for secure interoperation among heterogeneous applications which is what a CPHS is. Ensuring that a system is still secure while interacting with another system is an important issue in CPHS. Wang et al., (2010) suggest abstracting and modeling the workflow of a CPS and by extension the CPHS. A general workflow in CPHS comprises monitoring of physical processes and environment, networking including data aggregation and diffusion, computing which encompasses reasoning and analyzing the data collected during monitoring to determine whether the physical process satisfies certain pre-defined criteria, and actuation which executes the actions during the computing phase. Security objectives for CPHS include confidentiality, data and resource integrity, availability to ensure correct operation, and authentication of data, transactions, communications and people. Cyber-attacks typically occur during interactions between the physical process, networking, computing and actuation. The types of attack include eavesdropping, compromised-key attacks, man-in-the-middle attack, and denial-of-service attack. The cyber attackers include skilled hackers, disgruntled insiders, criminal elements, and nation-state terrorist groups (Wang et al, 2010). These researchers proposed a context-aware security framework that spans sensor security, cybersecurity, and control security. The latter comprises actuation security and feedback security. This framework provides a useful perspective to introduce measures in the CPHS to thwart cyber-attacks.

LEARNING, ADAPTATION AND TEAMING IN CPHS

Learning. Learning in CPHS can be for different purposes: learn about the operational environment; learn about the humans (e.g., intent, preference, where they can be trusted, where not), and learn about the cyber-physical system (e.g., availability, where it needs help), and learn how to mutually adapt. Learning in CPHS can exploit multiple sensor sources, can take a variety of forms, and satisfy different needs. The human and CPS can learn from each other, from the sensed operational environment, and from actions taken in that operational environment. Complicating factors are noisy sensors, partial observability, and disruptive events. Both offline and online learning play an important role in adaptive CPH systems. *Offline learning* is based on supervised learning. It is used to learn human information seeking policies, preferences and priorities (Madni et al., 1982). *Online learning* approaches include unsupervised learning and reinforcement learning. With supervised learning, the system learns general patterns from inputs and expected outputs given to the system by a "teacher." With unsupervised learning, the system learns patterns on its own without the aid of a "teacher." With reinforcement learning, the system takes actions for achieving a goal within its environment without the teacher telling it how close it is to that goal. Table 3 presents examples of learning in CPH systems.

Table 3. Examples of Learning in Adaptive CPH Systems

- CPS learns human information preference (offline)
  - supervised learning
- CPS infers human intent (online)
  - from noisy signals and context
- CPS learns human cognitive state
  - from physiological measures and contextual awareness
  - from correlating task performance with physiological measures

Adaptation. Adaptation occurs within adaptive CPHS for several reasons: to reduce human cognitive load, back up malfunctioning CPS, and respond to disruptions. There are different types of adaptation including: task re-allocation from humans to machines; task re-allocation from machines to humans; machine adapts to human priorities and preferences with changing context; and human adapts to machine limitations in specific contexts (Madni, 2017). Table 4 presents examples of adaptations, the triggering criteria, and the desired outcomes.

Table 4. Adaptation in Adaptive CPH Systems (Madni, 2017)

Adaptation Type	Triggering Criteria	Desired Outcome
Re-allocation of Task(s) from Human to Machine	human cognitive load exceeds threshold; fatigue; human error rate exceed threshold	manageable human cognitive load
Re-allocation of Task(s) from Machine to Human	novel situation unrecognizable by CPS; CPS request; CPS malfunction	superior handling of novel situations/ contingencies
Machine Adapts to Human	human preference structure and information seeking policy	increased S/N ratio information delivered to human especially under time-stress
Human Adapts to Machine	machine request to transfer control; change of context requires transfer of control	superior ability to deal with operational tasks and situation

Mutual adaptiveness is a key characteristic of high performance CPHS (Madni, 2017). Mutual adaptiveness is subject to human and CPS constraints and is facilitated by shared context awareness (Madni, 2017).

Teaming. A useful way to view the human and CPS in an adaptive CPHS is within a team construct, and then define teamwork for adaptive CPHS. Teamwork is the key to sustaining high performance especially in the face of disruptions. It is often said that, "A team of experts does not make an expert team." The challenge is to realize effective teamwork between the human and CP elements with full cognizance of human cognitive limitations and adaptation constraints and CPS implementation constraints.

FUNCTIONAL ARCHITECTURE OF ADAPTIVE CPHS

Figure 1 presents the functional architecture of an adaptive CPHS. As shown in the figure, the human-CPS interface is role-sensitive, context-aware, and user-adaptive (i.e., it presents information in accord with user preferences and priorities learned in offline supervised learning environment). The controller is adaptive and sensitive to human inputs and dynamic context changes. The human is in the role of supervisor/monitor or supervisor/controller depending on whether the human has the "conn" or the CPS has the "conn." The controller can pass the "conn" to the human voluntarily or based on human direction, dynamic function and task allocation based on pre-defined criteria and thresholds, as well as criteria for human backing up (i.e., taking over for) the CPS, and vice versa. The adaptive controller has facilities for multi-sensor correlation to disambiguate causes of variations in human behavior. It can re-task humans and cyber-physical elements, re-direct sensors, and modify control inputs to actuators based on external intelligence. Online machine learning, informed by user actions, sensor data, and actuator actions, can potentially enhance mutual adaptiveness between the human and cyber-physical elements.

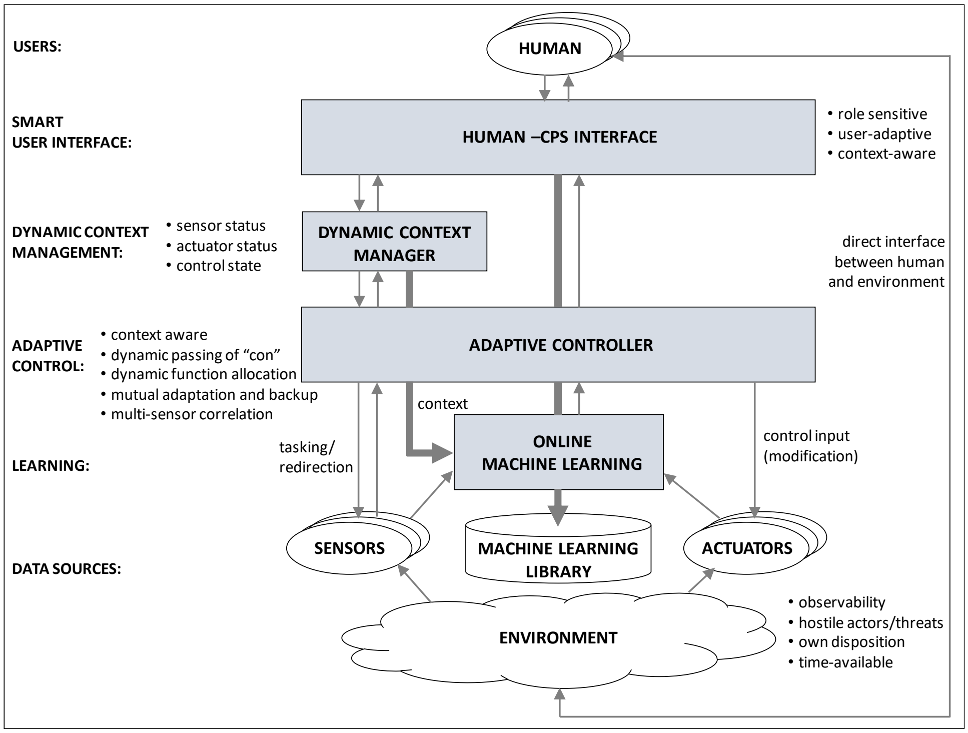


Figure 1. Functional Architecture of Adaptive CPHS

In adaptive CPHS, success criteria/metrics are associated with the range, rate and completeness of adaptation of the cyber-physical and human elements. Other key metrics, that are difficult to directly measure, but have "proxies" include shared contextual awareness, predictability, and trust.

KEY ELEMENTS OF TECHNICAL APPROACH

This section describes key elements of our technical approach. Shared Ontology is necessary to facilitate interoperation between human and CP Elements. Shared Governance during Collaborative Task Execution is required to ensure acceptable behavior of CPS. Human Intent Identification from EPS and Context intend to help CP elements to interpret human intention. Human Behavior Modeling is required to introduce human constraints and capabilities and facilitate CPHS Integration. Machine Learning is required to continuously improve adaptive behavior. These elements are discussed in more details next.

ADAPTIVE CPHS ONTOLOGY ELEMENTS: INITIAL SET

Below is the initial set of ontology elements with a brief description of each element.

- Human – person who will work with CP elements
- Role – container for person with requisite qualifications

- Task – activities performed by agent in a particular role
- Subtask – next level of decomposition of Task
- Agent – job performer (human or CP element)
- Cyber-Physical Elements (machine counterpart of human)
- Task Re-allocation – re-assignment of activities based on criteria
- Environment – set of factors that affect the operation of the CPHS
- Contingency Event – condition that causes task execution to deviate from routine
- Disruption – perturbation from external or internal sources that require CPHS to adjust/adapt operation.

Shared Governance and Task Execution

Responsibilities divided between human(s) and cyber-physical elements. During nominal operation, human is responsible for high-level planning and decision making and cyber-physical elements are focused on execution of detailed actions. During contingency situation, safety over-rides used to avoid hazardous actions/behaviors. Humans can intervene in CPS operation to redirect, take-over, or suspend operation. CP elements can also take over human task upon human request, or after human inactivity period exceeds a time threshold and CP queries during that period go unanswered by human.

Human Intent Identification: Possible Methods

Possible methods to use for human intent identification are:

1. Customize control HW and SW for individual human: this implies flexible HW and SW implementation that can be "trained" in the field. This requires special tools and training procedures to create scenarios for human in the CPHS, record physiological responses, and update SW tables and FPGAs

2. Ensure controller (HW, SW) has flexibility to work with any human agent, involves training the system like modern speech recognition.

3. Human explicitly communicates intent to controller HW and SW. For example, human employs hand-held controllers to change CPS behaviors. Downsides: of this method is that human is forced to focus on control, not high-level planning and decision making. It can be inconvenient if human has to carry equipment (flashlight, weapon). Usually humans don't multi-task well since there is potential for cognitive overload, stress, and divided attention.

Human Behavior Modeling

The purpose of HBM is to represent human interactions with CPS under various conditions such as cognitive overload, fatigue, high stress, and infrequent events. HBM requirements include determining the right level of fidelity based on domain, context, and task requirements, incorporating limitations of CP elements, incorporating human cognitive limitations, exhibiting adaptability and creativity, and defining criteria for when to intervene in CP processes.

The key concepts in human behavior modeling include: task (required knowledge/skills); person (knowledge/skillset, availability, location); role (qualification, training, testing, experience, location); and constraints (cognitive, attentional resources, geospatial).

Since not every aspect of a human needs to be modeled, models need to be appropriately scoped. For example, for cognitive tasks such as planning and decision-making, we do not need to model human kinematic constraints. But we most definitely need to model human cognitive limitations and adaptation constraints.

The level of abstraction of HBM varies with purpose. It ranges from general to specific. For example, a Smart Thermostat uses Hidden Markov Model to model occupancy and sleep patterns of residents to save energy – a high level behavior. On the other hand, impulsive injection of insulin uses math models for diabetes mellitus. In this case, a specific model determines the need for insulin injection by monitoring glucose level relative to threshold level for administering insulin – a low level model.

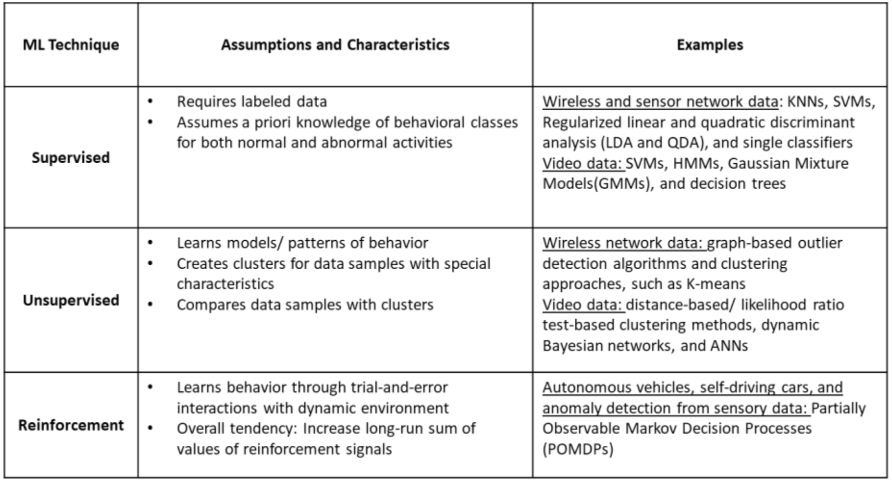
Model fidelity is based on model purpose, task/activity, interaction level with CPS, and sensitivity to environmental factors.

In sum, when performing HBM, two key questions need to be answered: What aspects of humans should be modeled (i.e., represented) for a specific adaptive CPHS? And Is there a methodological basis for determining appropriate sparse representation of a human for a particular class of CPHS?

MACHINE LEARNING: OPPORTUNITIES

Multiple sources of learning, sensors, networks, people. Complicating factors are partial observability, noisy sensors, disruptive events. Machine learning options can be supervised learning, unsupervised learning, reinforcement learning. Table 5 discusses these options.

Table 5. Machine Learning Techniques



ML Technique	Assumptions and Characteristics	Examples
Supervised	• Requires labeled data • Assumes a priori knowledge of behavioral classes for both normal and abnormal activities	Wireless and sensor network data: KNNs, SVMs, Regularized linear and quadratic discriminant analysis (LDA and QDA), and single classifiers Video data: SVMs, HMMs, Gaussian Mixture Models(GMMs), and decision trees
Unsupervised	• Learns models/ patterns of behavior • Creates clusters for data samples with special characteristics • Compares data samples with clusters	Wireless network data: graph-based outlier detection algorithms and clustering approaches, such as K-means Video data: distance-based/ likelihood ratio test-based clustering methods, dynamic Bayesian networks, and ANNs
Reinforcement	• Learns behavior through trial-and-error interactions with dynamic environment • Overall tendency: Increase long-run sum of values of reinforcement signals	Autonomous vehicles, self-driving cars, and anomaly detection from sensory data: Partially Observable Markov Decision Processes (POMDPs)

Illustrative Example and Prototype CPHS: Perimeter Security of C-130 Aircraft

Context: Forward Base Operations of C-130 aircraft security. C-130 parked on a landing strip adjacent to semi-urban environment with sparse roads. Parked C-130 offers adversaries ample attack opportunities. Perimeter security is provided by: video cameras and LWIR mounted on built-up structures in the vicinity, and unattended ground sensors (UGS) around the aircraft. The deplaning troops add additional UGS around the aircraft to further increase security. The commander in charge of aircraft perimeter has a quick set-up laptop with wireless connection to sensors and human/robotic sentries, real-time monitoring dashboard with facilities for anomaly detection, machine learning, selective region monitoring, and dynamic resource allocation.

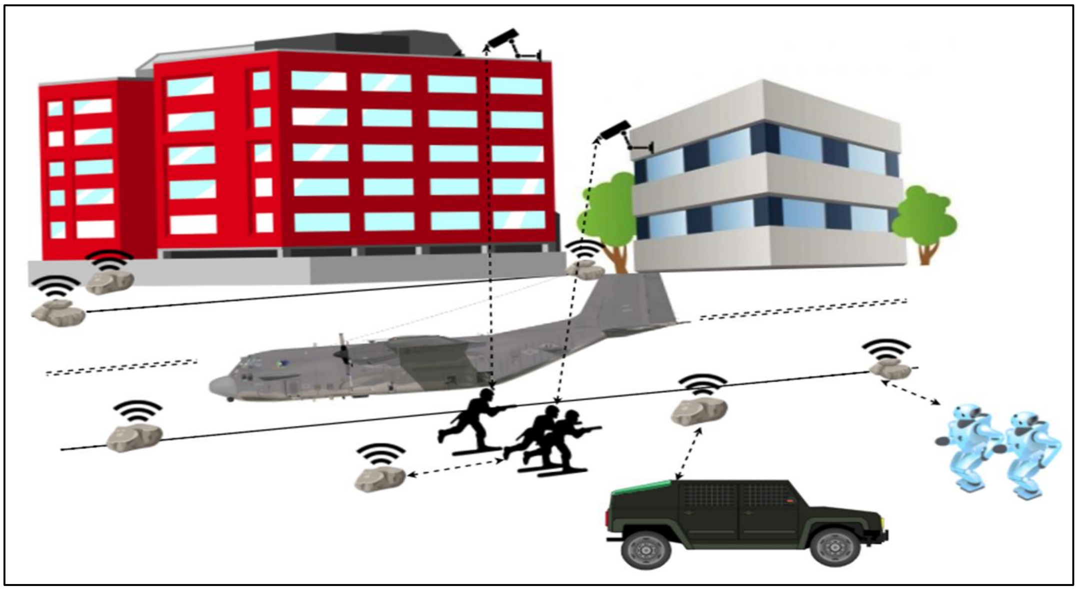


Figure 2. C-130 Aircraft Security

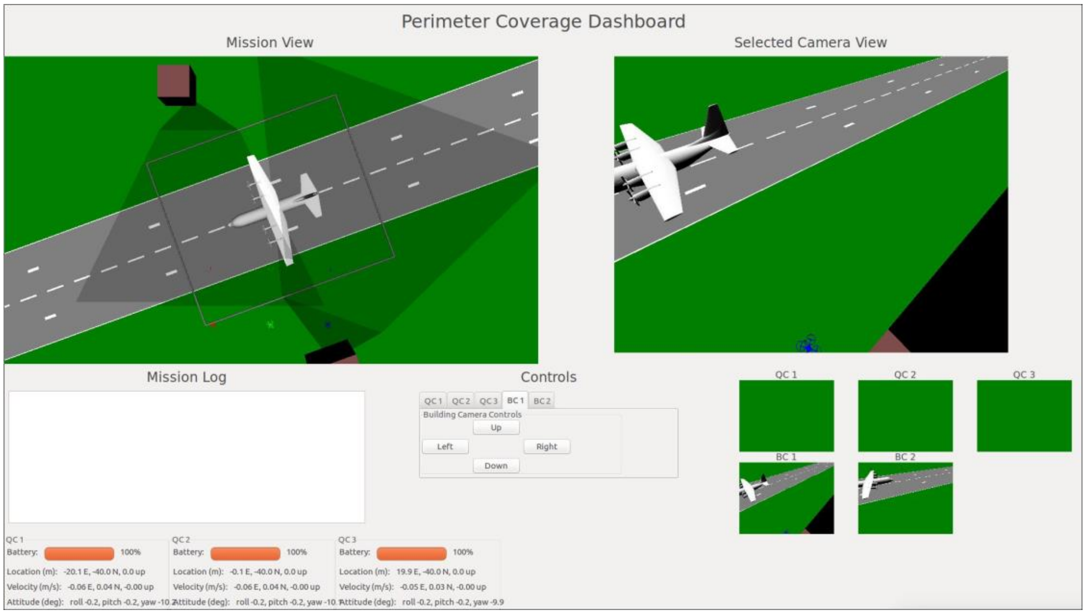
In this scenario (figure 2), a C-130 military transport is parked on a landing strip in the vicinity of a military outpost comprising several buildings. With security of the aircraft being paramount concern, the perimeter of the aircraft is secured by two kinds of surveillance assets: fixed-location, building-mounted cameras and downward-looking cameras mounted on airborne UAVs. For this is relatively small perimeter, the UAVs employed are quadcopters.

A simulator for this scenario is shown in figure 3. As shown in this figure, the Mission View is a plan view of the C-130 aircraft perimeter and surroundings. Two buildings are visible in this view. On each building a video-camera is mounted with views of the stationary aircraft from different directions. The shadows on the ground indicate the intersection of the viewing volume of each camera with the ground.

Three quadcopters, assigned to this surveillance mission, are ready for launch. These quadcopters can be seen on the ground at the bottom center of the mission view. There are five cameras in all (three quadcopters QC 1 – QC 3 and two building-mounted cameras BC 1 and BC

2). The views from each of the five cameras are shown at the lower right. The quadcopter cameras do not show anything because the quadcopters are still on the ground awaiting launch.

The Controls section in the bottom center of the simulator allows manual (human) control of the quadcopters and of the azimuth and elevation of the building cameras. The Selected Camera View shows the field of view for the camera corresponding to the currently selected control tab (BC 1 in figure 3).



QC 1
Battery: 100%
Location (m): -20.1 E, -40.0 N, 0.0 up
Velocity (m/s): -0.06 E, 0.04 N, -0.00 up
Attitude (deg): roll -0.2, pitch -0.2, yaw -10.2

QC 2
Battery: 100%
Location (m): -0.1 E, -40.0 N, 0.0 up
Velocity (m/s): -0.06 E, 0.04 N, -0.00 up
Attitude (deg): roll -0.2, pitch -0.2, yaw -10.1

QC 3
Battery: 100%
Location (m): 19.9 E, -40.0 N, 0.0 up
Velocity (m/s): -0.05 E, 0.03 N, -0.00 up
Attitude (deg): roll -0.2, pitch -0.2, yaw -9.9

Figure 3. Scenario Simulator

MULTI-ASSET CONTROL APPROACH

This scenario was chosen because it affords the opportunity to demonstrate three resilience aspects of the solution: adaptive coverage; human in the loop decision-making; and collaboration among multiple agents.

The problem is to control the collection assets (UAVs and fixed cameras) to optimize multi-sensor coverage of the aircraft perimeter. It is important to recognize a couple of key points about coverage:

- It is not adequate for a portion of the perimeter area to be within the field of view of a camera; the resolution (size of that area within the image) is also important. (Otherwise, it becomes possible to achieve complete coverage with a single quadcopter at very high altitude.)
- Where possible, coverage of a given area by multiple cameras is preferable to coverage by a single camera. This adds redundancy (an important resilience characteristic) and improves motion detection through stereo effects.

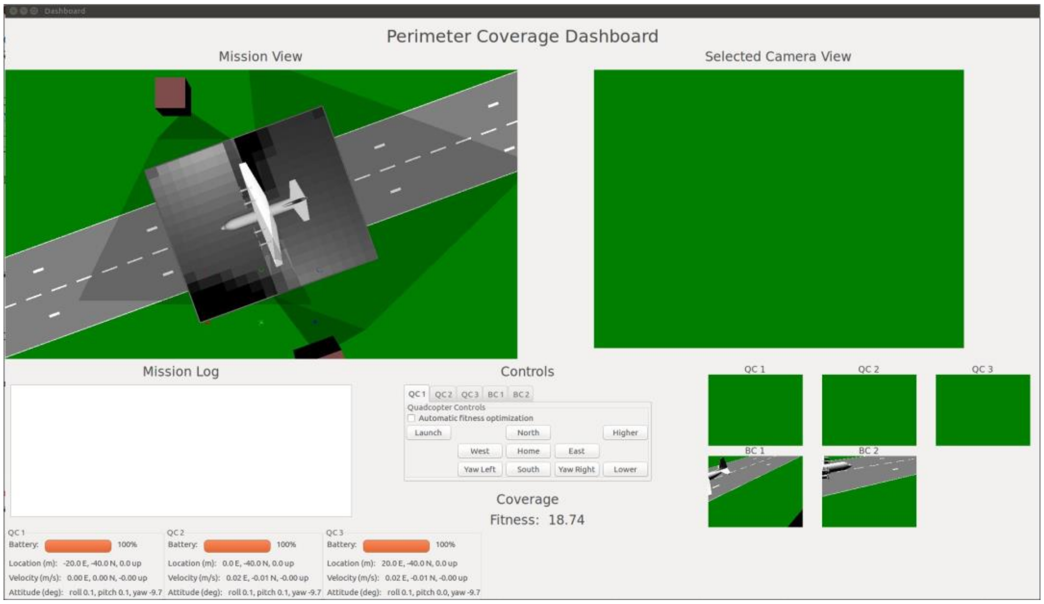
Taking these considerations into account, we employ a relatively simple fitness function to characterize perimeter coverage. The fitness function has the following properties:

- The coverage area is discretized into “tiles.” The fitness function considers the centroid of each tile and its intersection with the viewing volume of each camera.
- For each tile and each camera, a contribution to the fitness function is made if the centroid is visible to the camera, with the contribution increasing with higher resolution (i.e., decreasing with distance from the centroid to the camera).
- Optimization of coverage is analogous to maximization of the fitness function.
- The fitness value at each tile (i.e. the contribution of each tile to the overall fitness function) is maintained separately, forming an array of coverage values, which are used by quadcopter in their respective control algorithms as described below.
- The fitness function, which is computed centrally, is used in a distributed manner.

To flexibly allocate and move assets to optimize coverage, the algorithm employs multiple levels:

- **Multiagent control:** Upon launch, each quadcopter moves to an area designated by the human operator. When placed into automated mode, each quadcopter uses the centrally computed coverage array to determine the coverage at the edges of its field of view. When there is more coverage on one side than the other, the quadcopter moves towards the region with less coverage. Note that this approach allows independent movement of all quadcopters. However, the motion is coupled, since the coverage at the edge of one quadcopter’s field of view is affected by the motion of “nearest neighbor” quadcopters.
- **Adaptive:** When the situation changes, for instance due to malfunction or battery depletion of one UAV, the other vehicles move to adapt to the change.
- **Human-in-the-loop**: If multiagent control does not result in adequate coverage of the aircraft perimeter, a signal to the operator is raised to indicate failure of currently allocated assets to carry out the task. Then it is up to the human to take an appropriate action (e.g., launch one or more additional quadcopters).

The results of the foregoing strategy are shown below. Figure 4 shows the dashboard modified to show camera coverage of the discretized aircraft perimeter area, as well as the fitness function value (here, 18.7 with coverage only from the building-mounted cameras).



☐ Automatic fitness optimization

Fitness: 18.74

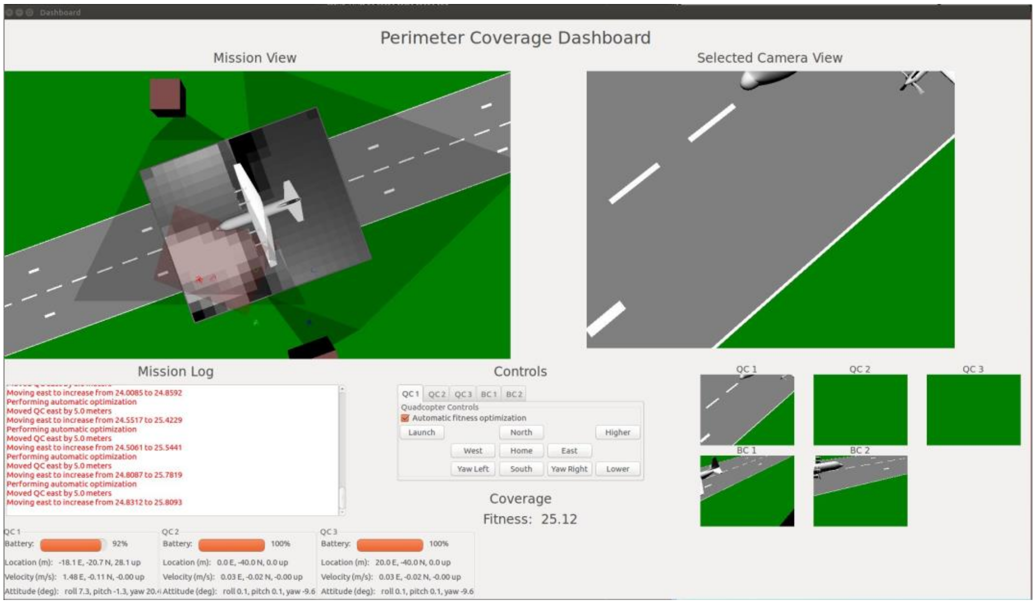
```
QC 1
Battery: 100%
Location (m):   -20.0 E, -40.0 N, 0.0 up
Velocity (m/s):   0.00 E, 0.00 N, -0.00 up
Attitude (deg):   roll 0.1, pitch 0.1, yaw -9.7

QC 2
Battery: 100%
Location (m):   0.0 E, -40.0 N, 0.0 up
Velocity (m/s):   0.02 E, -0.01 N, -0.00 up
Attitude (deg):   roll 0.1, pitch 0.1, yaw -9.7

QC 3
Battery: 100%
Location (m):   20.0 E, -40.0 N, 0.0 up
Velocity (m/s):   0.02 E, -0.01 N, -0.00 up
Attitude (deg):   roll 0.1, pitch 0.0, yaw -9.7
```

Figure 4. Dashboard Showing Coverage Area
(The quadcopters are not yet launched, so the coverage is due only to the building cameras.)

Figure 5 shows the results when one quadcopter is flying. Note that the control "Automatic fitness optimization" is checked, so that the quadcopter is moving in a manner to maximize the fitness function. The coverage area here shows the coverage due to the quadcopter. The messages in the mission log show the quadcopter's search for the optimal location.



```
Moving east to increase from 24.0085 to 24.8592
Performing automatic optimization
Moved QC east by 5.0 meters
Moving east to increase from 24.5517 to 25.4229
Performing automatic optimization
Moved QC east by 5.0 meters
Moving east to increase from 24.5061 to 25.5441
Performing automatic optimization
Moved QC east by 5.0 meters
Moving east to increase from 24.8087 to 25.7819
Performing automatic optimization
Moved QC east by 5.0 meters
Moving east to increase from 24.8312 to 25.8093
```

☑ Automatic fitness optimization

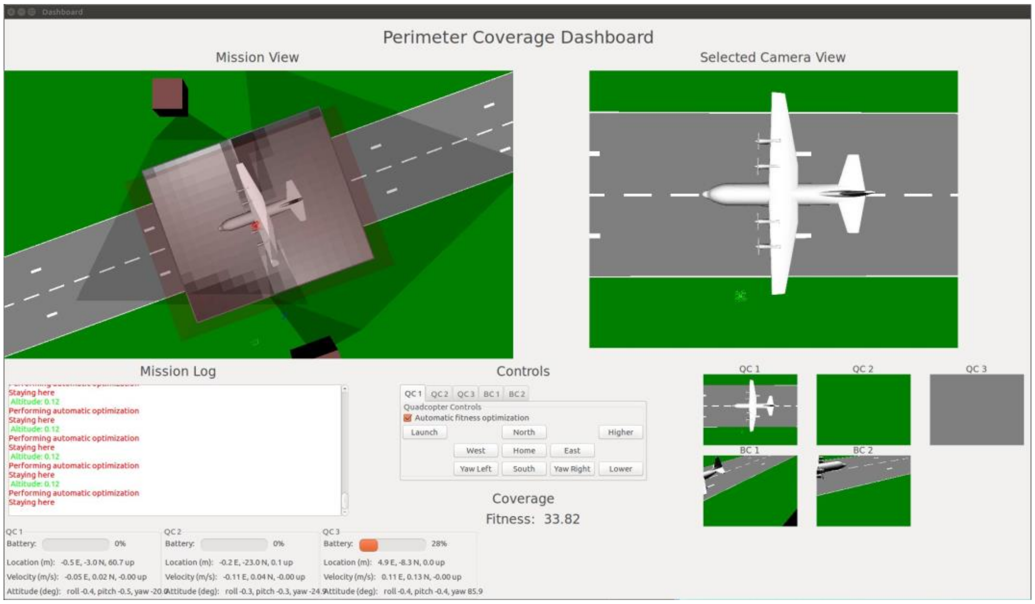
Fitness: 25.12

```
QC 1
Battery: 92%
Location (m):   -18.1 E, -20.7 N, 28.1 up
Velocity (m/s):   1.48 E, -0.11 N, -0.00 up
Attitude (deg):   roll 7.3, pitch -1.3, yaw 20.

QC 2
Battery: 100%
Location (m):   0.0 E, -40.0 N, 0.0 up
Velocity (m/s):   0.03 E, -0.02 N, -0.00 up
Attitude (deg):   roll 0.1, pitch 0.1, yaw -9.6

QC 3
Battery: 100%
Location (m):   20.0 E, -40.0 N, 0.0 up
Velocity (m/s):   0.03 E, -0.02 N, -0.00 up
Attitude (deg):   roll 0.1, pitch 0.1, yaw -9.6
```

Figure 5. Dashboard with one Quadcopter During Optimization of Fitness Function



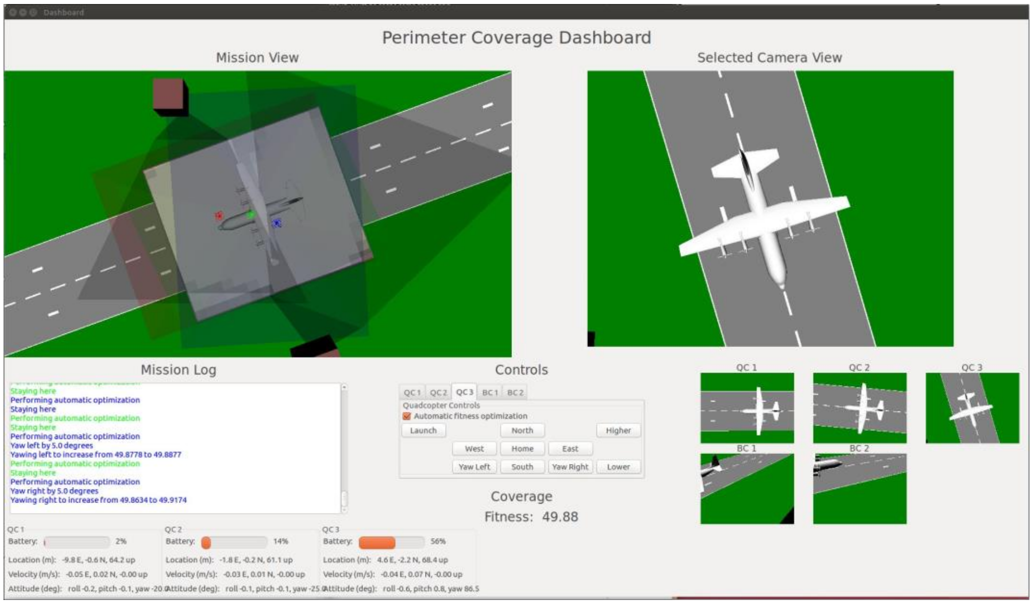
```
Staying here
 Altitude: 0.12
Performing automatic optimization
Staying here
 Altitude: 0.12
Performing automatic optimization
Staying here
 Altitude: 0.12
Performing automatic optimization
Staying here
 Altitude: 0.12
Performing automatic optimization
Staying here
```

Fitness: 33.82

```
QC 1                                          QC 2                                          QC 3
Battery:             0%                       Battery:             0%                       Battery:             28%
Location (m):   -0.5 E, -3.0 N, 60.7 up       Location (m):   -0.2 E, -23.0 N, 0.1 up       Location (m):   4.9 E, -8.3 N, 0.0 up
Velocity (m/s):   -0.05 E, 0.02 N, -0.00 up   Velocity (m/s):   -0.11 E, 0.04 N, -0.00 up   Velocity (m/s):   0.11 E, 0.13 N, -0.00 up
Attitude (deg):   roll -0.4, pitch -0.5, yaw -20.0Attitude (deg):   roll -0.3, pitch -0.3, yaw -24.9Attitude (deg):   roll -0.4, pitch -0.4, yaw 85.9
```

Figure 6. Optimal Location for a Single Quadcopter

Figure 6 shows the dashboard views after the single flying quadcopter has found the optimal position. Note that the quadcopter has climbed to 60 meters and yawed to -20 degrees to fit its field of view with the aircraft perimeter.



```
Staying here
Performing automatic optimization
Staying here
Performing automatic optimization
Staying here
Performing automatic optimization
Yaw left by 5.0 degrees
Yawing left to increase from 49.8778 to 49.8877
Performing automatic optimization
Staying here
Performing automatic optimization
Yaw right by 5.0 degrees
Yawing right to increase from 49.8634 to 49.9174
```

Fitness: 49.88

```
QC 1                                          QC 2                                          QC 3
Battery:             2%                       Battery:             14%                      Battery:             56%
Location (m):   -9.8 E, -0.6 N, 64.2 up       Location (m):   -1.8 E, -0.2 N, 61.1 up       Location (m):   4.6 E, -2.2 N, 68.4 up
Velocity (m/s):   -0.05 E, 0.02 N, -0.00 up   Velocity (m/s):   -0.03 E, 0.01 N, -0.00 up   Velocity (m/s):   -0.04 E, 0.07 N, -0.00 up
Attitude (deg):   roll -0.2, pitch -0.1, yaw -20.0Attitude (deg):   roll -0.1, pitch -0.1, yaw -25.0Attitude (deg):   roll -0.6, pitch 0.8, yaw 86.5
```

Figure 7. Optimal Locations for Three Quadcopters

In Figure 7, three quadcopters are shown in flight. They have deliberately separated to increase the quality of coverage for the entire perimeter. Note that the selected quadcopter has rotated its field of view to concentrate on the east end of the perimeter.

It should be noted that these results are strongly dependent on the form of the fitness function, which will continue to be refined in the next phase.

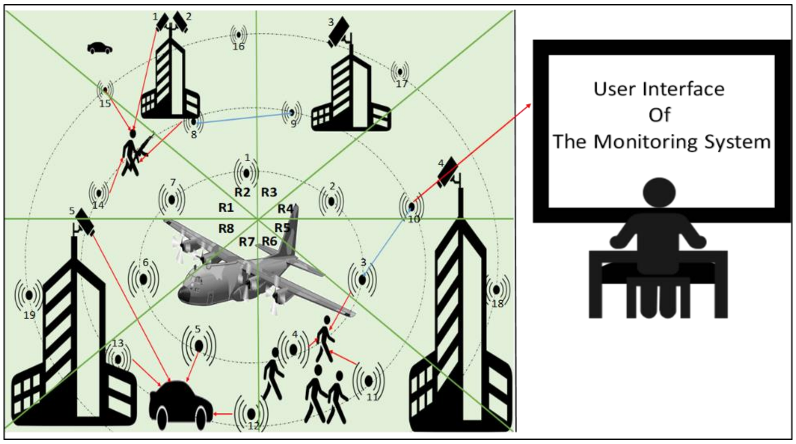
Human Roles and CPH Functions

CPH system comprises:

- Physical: laptop with smart dashboard software, sensors, robotic sentries; wireless connection to building mounted sensors and unattended ground sensors
- Cyber: monitoring, planning, visualization, resource allocation, machine learning software
- Human: commander in charge of maintaining aircraft security; UAV operator
- Human roles:
  - supervision, sensor tasking (what region to surveil); robotic/human sentry tasking (what region to patrol), intrusion monitoring, re-planning perimeter defense (incoming intelligence)
- CPS Functions:
  - learn commander priorities in various contexts; learn normal traffic and intruder patterns; follow patrol schemes; generate context-sensitive visualizations; issue alerts upon intrusion detection, reconfigure perimeter defense (standing orders)

Sample UI and User System Interaction

The monitoring system comprises 2 monitors (UI for humans-in-the-loop). The monitors provide real-time state and status info in color-coded format. Color-coded status of regions R1 through R8 is presented through the UI. Green region means region is safe, red means an intruder has been detected. Real-time views of the regions are providing data from security cameras. Detailed information on each region is provided based on actions on users. Monitor #1 provides overall status of individual regions, and real-time view based on updates from security cameras. Monitor #2 changes based on actions of human user taken through UI. When a region's display turns red, user clicks on that region's icon to acquire details. Monitor #2 provides detailed information on sensors, motion, location, camera, etc. - options: calling a security crew, turning on alarms, and reporting the incident



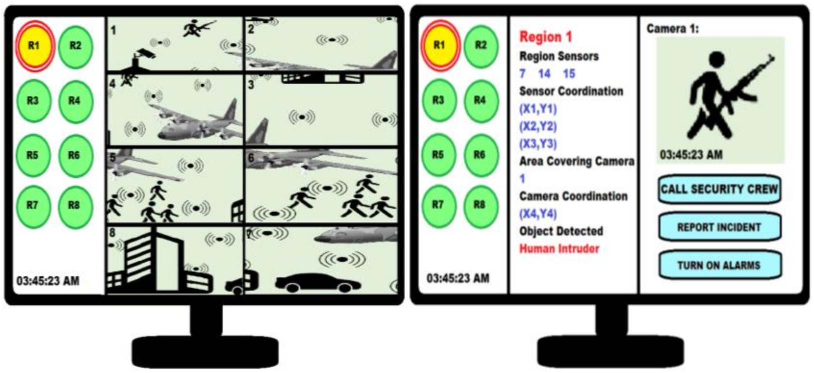


Figure 8. Monitoring System

Leverage of RT-166 Building blocks

For the experimentation testbed, we are leveraging the capabilities we created in RT-166. A prototype UAV whose actions are controlled by a decision-making algorithm such as POMDP. The specific criteria that we employed include:

- Ability to fly in an indoor laboratory as well as outdoors
- Large enough to carry a powerful onboard computer with a full suite of sensors (camera, GPS, IMU) which can run autopilot software as well as POMDP
- Support for open source software

Flying indoors meant that airplanes were ruled out as well as gasoline-powered motors. Battery-powered quadcopters thus became a clear choice. We selected a class of quadcopters with diameter of order 24 inches, with 1000 KV motors and 10-inch propellers, taking a LiPo battery with capacity of order 3000-5000 mAH. There is a wide variety of kits and parts for this class of vehicles, and since these are widely used by hobbyists, they are generally quite inexpensive.

For the onboard computer, a combination of Raspberry Pi 3 single-board computer and Navio2 flight controller was selected. The Raspberry Pi is a little smaller than a deck of cards but is a quad-core 1-GHz 64-bit CPU with 1 GB RAM, costing about $35. It runs a flavor of Debian Linux and so supports essentially all open-source software.

The Navio2 is a flight controller board that connects to the CPU via the GPIO pins. It carries the GPS, IMU, and magnetometer, as well as the PWM controllers for the motors. It is the most expensive component of the entire quadcopter but is essential for autonomous flight.

For the autopilot we selected Ardupilot, an open source program, because of its support for our hardware and because there is a wide variety of modes of operation as well as supporting modules. We particularly required *guided mode*, in which the UAV responds to external commands such as moving to a specified position, setting a specified velocity vector, or holding at a specified location and attitude. (An external command is one which originates outside the autopilot program. It can come from a ground station computer over a wireless communications link or from a different program running on the UAV CPU. Thus, guided mode is useful for fully autonomous maneuvers as well as centrally controlled operation.)

Ardupilot supports simulated quadcopters as well as actual ones. This enabled our prototype demonstration of control of 3 drones, two simulated and one real quadcopter. At present we have two complete operational quadcopters including flight controllers.

Indoor flight in our laboratory presents a special challenge because autonomous flight requires a solid GPS lock in the unmodified Ardupilot software. However, the GPS satellite signals are too weak in our laboratory to achieve this lock. Accordingly, one of our current tasks is to modify Ardupilot in order to use position and attitude information obtained from camera observations of multiple Aruco markers positioned on the walls and ceiling of our lab. We have experimentally demonstrated good accuracy of this technique but have not yet incorporated it into the flight software.

SUMMARY AND CONCLUSION

Next generation adaptive CPHS are a type of socio-technical systems in which computation, communication, and control are tightly integrated (Schirner et al., 2013). They comprise cyber, physical, and human elements and are capable of learning and adaptation based on operational context. Operational context is defined by the state of the environment, state of the human, and state of the cyber and physical components. State of the environment is described by attributes such as observability, threat level, and terrain and weather characteristics. The state of the human is described by cognitive load, fatigue level, vigilance level, and familiarity level with the task at hand. The state of the cyber-physical elements in the adaptive CPHS is described by computation and communication load, and level of knowledge of the task, environment, and the human counterpart. Next generation adaptive CPHS are safety-critical systems that can range from a small device to large-scale system-of-systems (SoS). The fact that humans can play a variety of roles in adaptive CPHS leads to increases in system complexity and vulnerability to cyber-attacks. Examples of adaptive CPHS are self-driving vehicles, adaptive energy grids, and healthcare enterprises.

Adaptive CPHS in the military need to operate safely in uncertain, dynamic environments with potentially hostile and deceptive agents. Adaptive CPHS face three key technical challenges: how to infer human intent; how to maintain shared context, and how to incorporate strong time semantics. Existing design tools are inadequate for modeling, analyzing and integrating adaptive CPHS for three main reasons. First, they address cyber, physical and human elements in isolation. Second, they tend to have overly simple human behavior models that do not reflect reality. Third, they do not address interactions between cyber, physical and human elements and their timing and synchronization constraints. A key challenge of adaptive CPHS is maintaining shared context in the face of disruptions. Flexible knowledge representation and machine learning are key to adaptive CPHS. Offline machine learning in the form of supervised learning can help the cyber-physical elements learn the preferences and priorities of humans across a range of contexts.

Online machine learning in the form of supervised learning and reinforcement learning can help the CPHS sustain high levels of performance in the face of disruptions.

The accomplishments of the first year include: a precise definition of adaptive CPHS; specification of a real world adaptive CPHS scenario of interest to DoD; development of a testbed to prototype adaptive CPHS; and use of the testbed to create a preliminary prototype of an adaptive CPHS. The prototype showcases the capabilities of an adaptive CPHS for maintaining perimeter security of a parked C-130 aircraft. The adaptive CPHS in this case comprises unattended ground sensors, fixed and mobile sensors, surveillance and adaptive planning and execution dashboard, mission commander who commands and controls distributed assets using the capabilities of the dashboard, and human sentries who change patrol patterns based on the mission commander's directives. The prototype demonstrates the dynamic coverage of the aircraft perimeter based on optimizing coverage using a fitness algorithm.

REFERENCES

Madni, A.M. Next Generation Adaptive Cyber-Physical-Human Systems, SERC MBSE Colloquium, Washington D.C. July 12, 2018

Madni, A.M., Madni, C.C. and Sievers, M. "Adaptive Cyber-Physical-Human Systems," 2018 INCOSE International Symposium, July 7-12, 2018.

Gelenbe, E., Gorbil, G. and Wu, F. "Emergency Cyber-Physical-Human Systems," *International Conference on Computer Communications and Networks* (ICCCN), Aug 2012.

Inagaki, T. "Adaptive Automation: Sharing and Trading of Control," *Handbook of Cognitive Task Analysis*, 8: 147-169, 2003.

Kay, M., Choe, E.K., Shepherd, J. Greenstein, B., Watson, N., Consolvo, S., and Kientz, J.A. "Lullaby: A Capture and Access System for Understanding the Sleep Environment," *UbiComp*, 2012.

Lu, J., Sookoor, T., Srinivasan, V., Gao, G., Holben, B., Stankovic, J., Field, E., and Whitehouse, I. "The Smart Thermostat: Using Occupancy Sensors to Save Energy in Homes, *SenSys*, 2010.

Madni, A.M. "Integrating Humans with Software and Systems: Technical Challenges and a Research Agenda," *Systems Engineering*, Vol. 13, No. 3, pp. 232-245, Autumn (Fall) 2010.

Madni, A.M. "Integrating Humans With and Within Software and Systems: Challenges and Opportunities," (Invited Paper) *CrossTalk, Journal of Defense Software Engineering*, May/June 2011, "People Solutions."

Madni, A.M. “Generating Novel Options During Systems Architecting: Psychological Principles, Systems Thinking, and Computer-Based Aiding,” *Systems Engineering*, Volume 17, Number 1, pp. 1-9, 2014.

Madni, A.M. “Mutual Adaptation in Human-Machine Teams,” Intelligent Systems Technology, Inc., Document No.: ISTI-WP-02-012017, January 11, 2017.

Madni, A.M., Samet, M.G., and Freedy, A. “A Trainable On-Line Model of the Human Operator in Information Acquisition Tasks,” *IEEE Transactions of Systems, Man, and Cybernetics, Special issue on Human Factors in Computer Management of Information for Decision Making*, Vol. SMC-12, No. 4, July/August, 1982, pp. 504-511.

Madni, A.M. and Sievers, M. “Model Based Systems Engineering: Motivation, Current Status and Research Directions,” accepted for publication in *Systems Engineering*, *Special Issue on Model-Based Systems Engineering*, 2018.

Munir, S., Stankovic, J.A., Liang, C.M., and Lin, S. “Cyber Physical System Challenges for Human-in-the-Loop Control,” *8th International Workshop on Feedback Computing*, USENIX Federated Conference, June 25, 2013.

Neches, R. and Madni, A.M. “Towards Affordably Adaptable and Effective Systems,” *Systems Engineering*, Vol. 16, No. 2, pp. 224-234, Summer 2013.

Robinson, R.M., Scubee, D.R.R., Burden, S.A., and Sastry, S.S. “Dynamic Inverse Models in Human-Cyber-Physical Systems,” *Proceedings Micro-and Nanotechnology Sensors, Systems and Applications VIII*, SPIE Defense & Security, vol. 9836, 2016.

Schirner, G., Erdogmus, D., Chowdhury, K., and Padir, T. “The Future of Human-on-the-Loop Cyber-Physical Systems, *Computer*, 46, 1(2013), 36-45, 2013.

Sheridan, T. B. *Telerobotics, Automation, and Human Supervisory Control*. MIT Press, Cambridge, 1992.

Sowe, S.K., Simmon, E., Zettsu, I., deVaulx, F., and Bojanova, I. “Cyber Physical-Human Systems: Putting People in the Loop, *IEEE Computer Society IT Professional*, Vo., 18, Issue 1, 2016.

Wang, E.K., Ye, Y.,Xu, X., Yiu, S.M., Hui, L.C.K., and Chow, K.P. “Security Issues and Challenges for Cyber Physical System,” *2010 IEEE/ACM International Conference on Green Computing and Communications* & *2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing*, IEEE Computer Society, pp. 733-738.