SYSTEMS ENGINEERING RESEARCH CENTER

Next Generation Adaptive Cyber Physical Human Systems

Technical Report SERC-2019-TR-013

September 4, 2019

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

Shatad Purohit, 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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF (TABLES, SEQUENCES)

ABSTRACT

Cyber-Physical-Human Systems (CPHS) are a class of safety-critical, sociotechnical systems in which the interactions between the physical system and cyber elements that control its operation are influenced by human agents. The key distinguishing feature of CPHS are that human (agents) can intervene in cyber-physical system (CPS) task execution to redirect the system, or supply needed information, not just to assume full control, or exercise manual-override of CPS processes or tasks. CPHS typically allow other systems, devices, and data streams to connect/disconnect as needed during mission execution. In adaptive CPHS, humans collaborate with the cyber-physical elements to jointly accomplish tasks and adapt as needed to changing contexts to accomplish mission goals. The adaptation exploits prior knowledge and new knowledge gleaned from online machine learning while accommodating human cognitive constraints. A DoD-relevant problem scenario concerned with maintaining physical security of a stationary transport aircraft using building mounted cameras and a team of quadcopters that collectively maintain perimeter coverage is used to demonstrate the capabilities of the adaptive CPHS. The exemplar scenario is used to illustrate the interactions between the human and the cyber-physical system, as well as ongoing adaptations to restore loss of perimeter coverage arising from ongoing disruptions (e.g., loss of a quadcopter). This final report presents our accomplishments on 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. CPHS are a purposeful combination of computational algorithms, physical components, and humans (agents). The key distinguishing feature of CPHS are that human (agents) can intervene in cyber-physical system (CPS) task execution to redirect the system, or supply needed information, not just to assume full control, or exercise manual-override of CPS processes or tasks. CPHS typically allow other systems, devices, and data streams to connect/disconnect as needed during mission execution. In adaptive CPHS, humans collaborate with the cyber-physical elements to jointly accomplish tasks and adapt as needed to changing contexts to accomplish mission goals.

Cyber-Physical-Human (CPH) systems today encompass a wide variety of systems including smart grid, smart manufacturing, smart homes, self-driving vehicles, emergency response systems (Glenebe 2012), and smart medical devices. An important challenge in the design of CPH systems is assuring compatibility in shared human-CPS decision making. This is a challenging modeling and integration problem because of the variability in human behavior, lack of shared contextual awareness and CPS limitations. 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 a few major universities is beginning to look at the development of frameworks for complex human-CPS modeling and analysis (Madni and Sievers, 2018). For example, researchers at CMU's Robotic Institute are conducting research in understanding integrated human-CPS behavior. They are attempting to develop fundamental principles and algorithms that can serve as a foundation for provably safe, robust hybrid control systems for mixed human-CPS operations. They are also working on methods for developing analytical human models that incorporate cognitive abilities and limitations and reflect that in interactive human control of CPS elements. Similarly, researchers at UC Berkeley are working on predictive methods for guaranteeing performance of CPH systems (Robinson et al., 2016).

Adaptive CPHS are CPHS that are capable of adapting to systemic malfunctions and external disruptions during operation using pre-determined rules and machine learning techniques. Applied 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). In particular, 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, as well as any instrumented device that require adaptive response based on context.

This final report presents our accomplishments in year two of our ongoing DoD SERC-sponsored research project in next generation adaptive CPH systems being conducted at the University of Southern California.

CHALLENGES IN ADAPTIVE CPHS DESIGN

As noted earlier, 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) (Schirner et al 1992, Sowe et al 2016). Adaptive CPHS are CPHS that are capable of adapting to systemic malfunctions and external disruptions during operation using pre-determined rules and machine learning techniques (Madni 1985). An adaptive CPHS needs to create and capitalize on the synergy between the human and CPS elements. There are several challenges that need to be overcome to create adaptive human-CPS teams (Madni, 2010; Madni, 2011). These include:

- *Performance Degradation*: occurs with sustained high cognitive load and/or fatigue
- *Unpredictability*: arises from human variability in task performance
- *Human Reluctance*: humans need to be incentivized to perform as a team
- *Misperception of Humans*: humans 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*: these need to be circumvented during task performance and especially during dynamic function allocation
- *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 assigned 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*: need to be allocated to CPS (CPS does not tire; can be augmented by additional CPS elements, if overloaded)
- *Human Behavior Modeling*: scope and perspectives are determined by model purpose and context; scope is determined by the questions that the model needs to answer
- *Bi-Directional Learning*: needed for effective joint performance (e.g., machine learns human preferences and priorities offline; human learns machine limitations and capabilities online and offline
- *Shared Decision Making*: exploit respective strengths of human and CPS while circumventing their respective limitations (Madni, 2014)
- *Context Recognition*: CPS needs to recognize context to determine how well (i.e., to what degree, how fast) humans can adapt in a particular context
- *Role Switching*: CPS need to keep track of multiple human roles and human role switches during task performance

There are other limitations that can surface during task execution. For example, the CPS may not be aware of the human's awareness of certain environmental factors that only 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 does 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 information 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 those tasks exclusively human performed tasks.

Two of the more important challenges in adaptive CPHS are learning and adaptation; and defining human roles in adaptive CPHS. These are discussed below.

Learning. Learning in CPS 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). Learning in CPS 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 CPHS. *Offline learning*, based on supervised learning can be used to learn human information seeking policies, preferences and priorities (Madni et al., 1982). *Online learning* includes both 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 1 presents examples of learning in CPHS.

Table 1. Examples of Learning in Adaptive CPH Systems

- CPS learns human information preference (offline)
  - supervised learning
- CPS infers human intent (online)
  - from noisy electrophysiological sensors and context
  - supervised and reinforcement learning
- CPS learns human cognitive state
  - from electrophysiological measures
  - from correlating task performance with electrophysiological measures

Adaptation. Adaptation within adaptive CPHS occurs for several reasons: reduce human cognitive load; back up malfunctioning CPS; and respond to disruptions. Adaptation can take a variety of forms: 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, Madni et al 2018). Table 2 presents examples of adaptations, the triggering criteria, and the desired outcomes.

Table 2. 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	change in 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

Human Roles in Adaptive CPHS. Human and machine strengths and limitations have been extensively addressed in the literature (Madni, 2010; Madni, 2011). In light of this research, several adaptive CPHS-related questions need to be answered: 1) What roles can 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? (Table 3).

Table 3: 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)

ADAPTIVE CPHS: AREAS OF INVESTIGATION

INTEGRATING HUMANS (AND/OR HUMAN BEHAVIOR MODEL) AT DIFFERENT LEVELS IN THE CONTROL LOOP

In adaptive CPHS, humans can perform a variety of roles (e.g., supervisor, collaborating peers). These roles imply that the human can be on-the-loop or in the loop. When in the loop, the human can be in the planning loop or the control loop. Furthermore, a human model can be explicitly or implicitly part of the overall system model to ensure that human cognitive (and other limitations) are accounted for in planning, decision-making and control. It is important to recognize that not all aspects of a human come into play in joint task performance. Therefore, only those aspects that apply need to be modeled (i.e., the other aspects can be ignored without compromising joint system performance). For example, if the human is involved in purely perceptual and cognitive tasks, then there is no need to model the kinematic aspects of the human. The questions that arise are whether or not appropriate sparse representations can be defined for specific classes of tasks. If this were possible, then we could simplify both the modeling effort and the computation load. Given the scope of our project, we will only tangentially address this point which deserves a dedicated research project.

BI-DIRECTIONAL ADAPTIVE CPH DECISION SYSTEM

Ultimately, our goal is to demonstrate the design of an adaptive CPHS that minimizes human error and oversight. With this goal in mind, we have pursued advances on the following research fronts: testbed design and instrumentation; smart dashboard implementation; and adaptive CPHS interaction design.

The main goal to architecting a bi-directional adaptive cyber-physical-human decision system is to achieve joint goals while minimizing human error and oversight. As such the knowledge and decision support system design must ensure that the: (1) human is not cognitively overloaded; (2) human does not have to monitor infrequent events; (3) human and CPS are not assigned tasks they do poorly; and (4) human and CPS are assigned tasks that they do well. As a result, the system approach must: (1) define a context ontology including context triggers; (2) maintain shared context between human and CPS; and (3) manage context to ensure effective decision-making (Ingaki 2003, Madni 1988a, Madni 1988b) . Figure 1 partitions the task performance space in terms of human and CPS strengths and limitations.

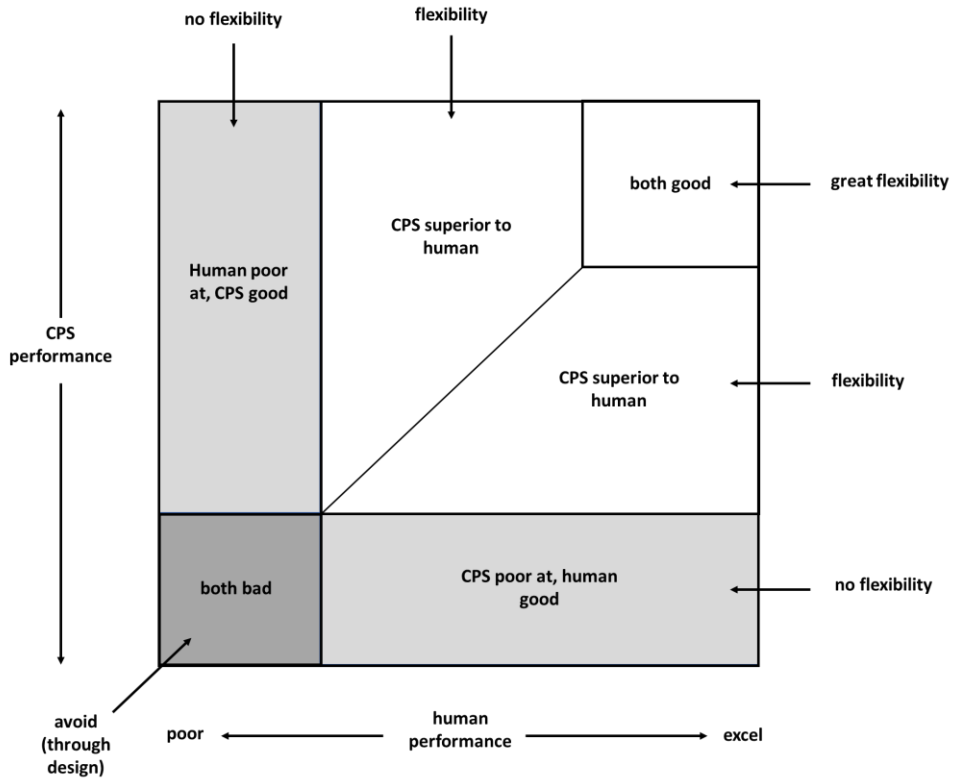

Figure 1. Understanding Human-CPS Function Allocation (Madni, A.M., 2019)

As shown in Figure 1, humans and CPS have different strengths and limitation. There are tasks that: (1) neither does well (rapid risk assessment); (2) both do well (option selection); (3) human does better than CPS (novel option generation); (4) CPS does better than human (recall known options); and (5) better together than either alone (shared perception). These strengths and limitations imply that in dynamic task allocation heuristics should avoid tasks that neither the human or CPS do well, capitalize on tasks that both do well, exploit the flexibility afforded by tasks that human do better than CPS, and recognize the context for which CPS performs tasks better than human (Madni 2011, Madni 2017).

ONTOLOGY-ENABLED INTEGRATION OF ADAPTIVE CPHS

To integrate the cyber-physical-human system and to further investigate the interdependencies among its components the following ontology is created. Figure 2 shows the initial ontology elements. Ontologies allow to formally define the elements within the domain and facilitate the understanding of the problem nature. Furthermore, ontologies can be used to reason about system behavior(Orellana 2012).

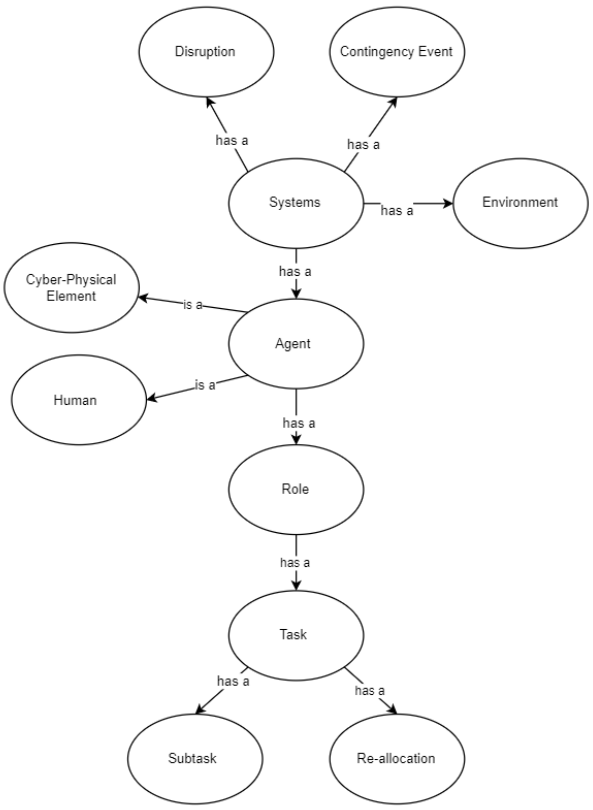

Figure 2. Key Elements in Adaptive CPHS Ontology

ILLUSTRATIVE EXAMPLE: PERIMETER SECURITY OF C-130 AIRCRAFT

We implemented a dashboard for our illustrative example. The underlying ontology employed within the dashboard is METT-TC (Madni, 2002), a mnemonic used by the U.S. Army to help commanders remember and prioritize what factors to analyze during operations planning. The mnemonic METT-TC stands for mission, enemy, troops, terrain (and weather), time available, and civilian. Each of these terms will have a window assigned to them on the dashboard. Since not all terms will apply to all missions, the dashboard will be tailorable and context-sensitive.

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.

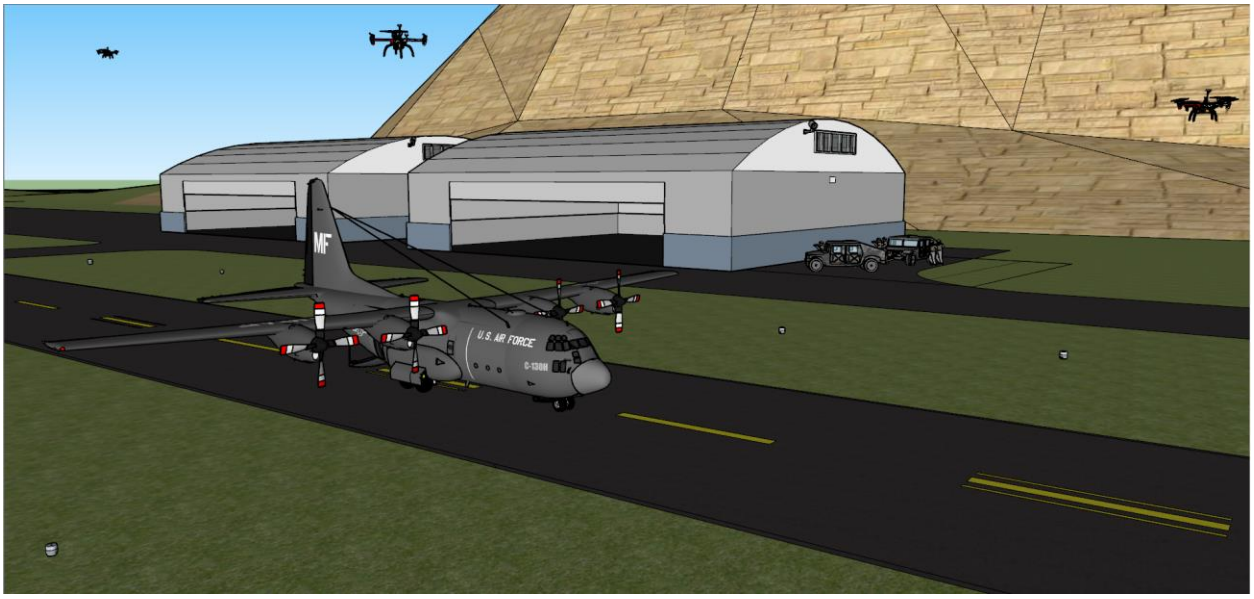

Figure 3. C-130 Aircraft Security

In this scenario (figure 3), 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.

ACCOMPLISHMENTS

The overall goal for this effort was to investigate innovative approaches for developing next generation adaptive CPHS in which human(s) and CP elements collaborate in joint task performance and adapt as needed to respond to operational contingencies and unexpected situations. In year 2 of this effort, we have made accomplishments in four areas: experimentation testbed, smart dashboard, multi-asset control approach, and agent-in-the-loop learning. These are essential components of the experimentation testbed. Our work has centered on the aircraft perimeter defense problem as an exemplar. From the METT-TC viewpoint, the work to this point has addressed mission, time, enemy, and available troops. We have explored ways of extending the mission dashboard to allow:

- Detection of threats approaching perimeter of airfield
    - Threats include enemy soldiers and or any unidentified moving object (e.g., animals)
- Tracking of threats using available cameras (mobile or building-mounted)
- Agent-in-the-loop learning from human supervisor (machine learning-enabled)
- Motion tracking and feature extraction of any moving objects
- Extended the experimentation testbed using a distributed, networked architecture

EXPERIMENTATION TESTBED

The experimentation testbed is being created to serve the needs of concept developers, systems engineers, system operators, and test engineers. It will have rudimentary capabilities to verify and enforce physical properties, build time and run-time environments, and libraries of scenario and system parts. The testbed is intended to support exploration of concepts, models, heuristics, and algorithms in a variety of simulated operational scenarios subject to a variety of injects.

The Testbed is being designed to support studies of different human roles and their integration with the cyber-physical elements. Human roles can be on-the-loop or in-the-loop. In-the-loop human roles can vary from high level control to low level control. The testbed functional architecture will eventually comprise:

- CPHS models and operational scenarios
- Sensors models and interface to physical sensors
- Library of starter kit system models, scenarios, and scenario injects
- Process models (development, testing)
- Human behavioral models (different levels of fidelity)
- Library of machine learning algorithms
- Build-time user interface for graphical system modeling and verification
- Run-time user interface comprising a smart dashboard
- Facilities for context management
- Facilities for data collection from simulated and physical sensors

CPHS have certain unique requirements. First, since CPHS tend to be safety-critical systems, we need facilities to model such systems. Second, CPHS architectures tend to combine third-party components and legacy components from previously deployed systems. As such, some of their components are fully verified under certain operating conditions that may or may not apply in their reuse. Third, CPHS are subject to unreliable interactions (e.g., sporadic or incorrect sensor inputs, control commands are not always precisely followed) because they interact frequently with the physical world. Fourth, CPHS are increasingly more susceptible to threats. Therefore, the testbed will provide:

- *Probabilistic system models with in-use learning facilities.* These models will begin with incomplete system representation and progressively fill in details of the model with incoming evidence and through learning of system and environment states.
- *Enforceable physical properties* are a key requirement because adaptive CPHS execute in and interact with dynamic and unpredictable physical environments. Certain aspects of the CPHS must remain impervious to changes in the dynamic environment. The testbed can be used to verify that.
- *Off-the-shelf components* are an integral part of adaptive CPHS. Adaptive CPHS comprise heterogeneous systems built from off-the-shelf components that communicate with each other across multiple networks. Because off-the-shelf components are commonly used in

CPHS, the testbed will support both physical presence of these components and their virtual models.
- *Support for safety-critical systems implementation* through, for example, executable, real-time system models that detect safety problems and then shut down.

The testbed will eventually support various analyses including CPHS model verification, system behavior validation, trade-space analysis and visualization, change propagation analysis, and system performance analysis especially in the face of disruptions. The testbed currently supports model verification and system validation in simulated operational settings.

In the past performance period, we have extended the testbed so that the simulation runs on multiple machines using a distributed, networked architecture. We have demonstrated two adversarial controllers, each running on its own machine and connecting to a third machine that maintains the common model of the shared world. The adversarial controllers are referred to as the "C130 dashboard," that controls the assets for the perimeter defense, and the "soldier dashboard," that controls enemy soldiers with the goal of penetrating the perimeter. The shared world is referred to as the "world server."

SMART DASHBOARD

The behavior of the adaptive CPHS is monitored and influenced through a smart dashboard with context-sensitive displays. The purpose of the dashboard is to allow users to:

- Understand the system and its operation from their respective perspectives
- View system behavior (vulnerabilities, violations) in graphical terms within DoD-relevant problem scenarios
- Interact with and explore system behavior by changing system parameters that create stress conditions at or near system performance boundaries

The smart dashboard is intended to hide complexity while conveying the necessary information to the users. Some of the key techniques that can be employed include: visual portrayal of quantitative information, flagging constraint violations using color codes, sound alerts, and graphical displays to show for example threshold violations; drawing attention to specific system states using cues, color codes, and symbols; and generally allowing the user to monitor the system within multiple contexts to develop a better understanding (Madni, 2012; Madni et al, 2014). The key benefits of an interactive smart dashboard are superior understanding of the system and operational environment.

An exemplar dashboard that has been prototyped for the "parked aircraft perimeter security" is shown in figure 4. 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. Moreover, key attributes and their levels associated with the mission and operations are shown.

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 4).

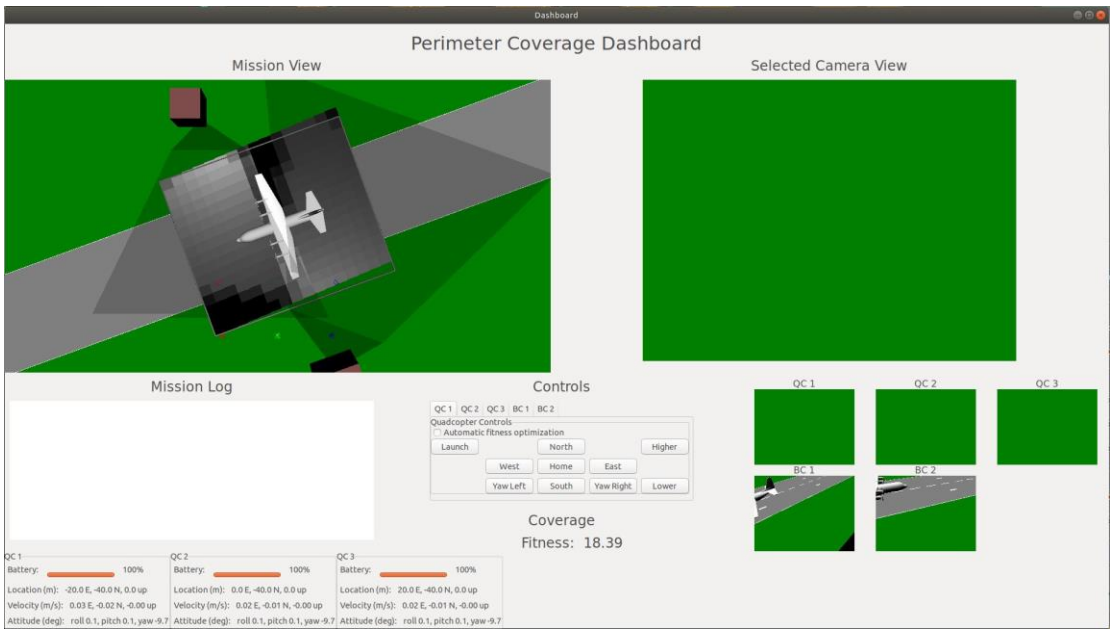

Figure 4. Scenario Simulator

Camera model

In the simulations, we have assumed the asset cameras to have performance similar to inexpensive hobby-grade circuit board cameras, and in particular the PiCam (the mini camera video module for the Raspberry Pi family of single-board miniature computers). The PiCam has a view angle of 68.9˚ in the horizontal direction, with an aspect ratio of 1.33. Multiple resolutions can be selected but 40 frames per second can be recorded with a 1640- by 1232-pixel resolution. We have modeled the camera as an ideal pinhole camera, so it is characterized by a standard projection matrix. Actual PiCams have significant fisheye distortion, but in our experimental work our standard procedure is to remove the distortion using a previously obtained calibration dataset, measured for each individual PiCam. The images so obtained conform to the ideal pinhole model with subpixel accuracy in the central third of the image, and with accuracy about two pixels at the extreme edge of the image. Thus, our simulated model is a very good model of the actual PiCam with distortion removal.

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.

- **<u>Human-in-the-loop</u>**: 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).

As an example, in figure 5, 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.

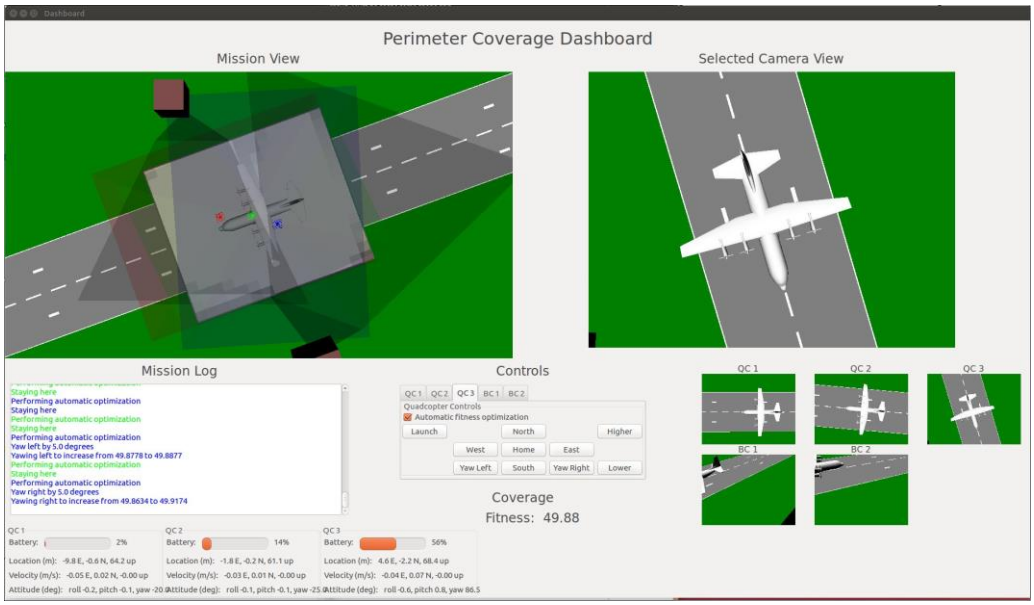

Figure 5. Optimal Locations for Three Quadcopters

We have added a threat analysis capability to the C130 dashboard. This capability employs image processing to identify unknown moving objects near the grounded aircraft. The analysis is done on video frames from the simulated cameras (quadcopter-mounted or building-mounted).
It should be noted immediately that the C130 dashboard "knows" already where the enemy soldiers are, through querying the world server, and displays them in the mission view and in the camera views. However, this information is not used in the threat analysis, i.e., the analysis does not cheat. Instead it uses only the information from available sensors, in this case the camera assets. The method developed here can be directly applied to a laboratory demonstration involving actual fixed and quadcopter-mounted cameras, for which the enemy soldiers would be actual mobile robots.

Motion detection

To detect and track motion, we use image analysis using the open-source OpenCV computer vision software library. Because in our problem, the aircraft perimeter is seen from widely different vantage points (since the quadcopters move to different locations including altitudes), identification of key points must be done in a scale-invariant fashion. Accordingly, from the various techniques of feature identification, we have selected SIFT (Scale-Invariant Feature

Transform). This method works on a grayscale image, so the full-color image obtained from the camera must be converted to grayscale.

Optical flow is estimated using the Lucas-Kanade (LK) pyramid method, implemented in the OpenCV calcOpticalFlowPyrLK function. It should be noted that this does not result in a pixel-by-pixel motion estimation. This is because the key points identified by SIFT (or other feature extractors) are typically points where the image is changing in some locally maximal way. This is seen in figure 6, which shows a camera image with the SIFT-identified key points marked with white dots. Also, the key points concentrate at corners and extremities, while uniform areas (e.g., runway, grass) are free of key points.

The result of optical flow is a set of vectors which point from the pixel location of a given key point in one image to the pixel location of the same key point in a succeeding image. If the key point is part of a moving object, the two locations are different, and the vector has positive length. (As discussed above, the motion can be due either to object motion or to camera motion, or both.)

Figure 7 shows the results of the LK method for an image which is moving due to camera motion. The camera is mounted on a quadcopter that is ascending, so the image points are moving inward.

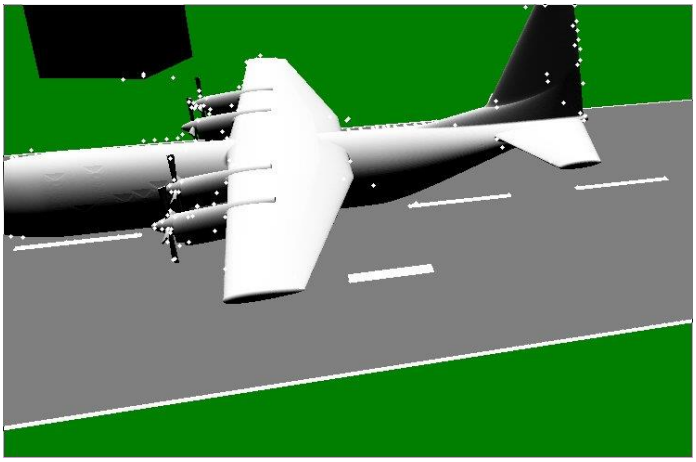

Figure 6. SIFT Key Points, Taken from an Image from Stationary Camera

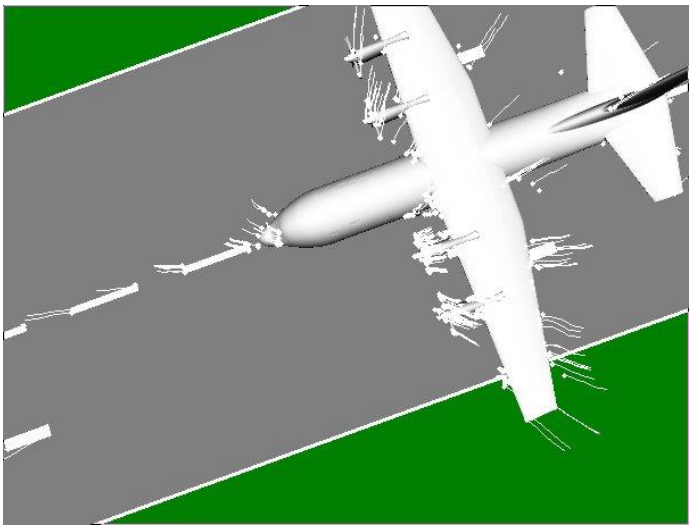

Figure 7. Optical Flow in An Image from a Moving Camera

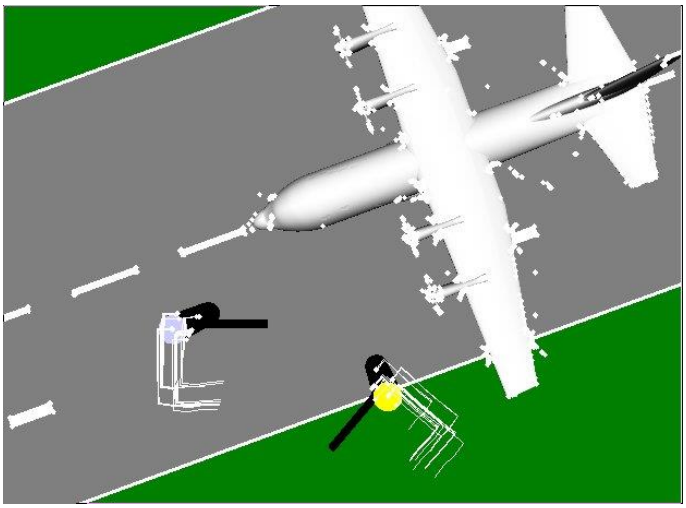

Figure 8. Motion of Enemy Soldiers

In figure 8, two simulated enemy soldiers are seen. They are each moving along a small square; the one shown at left is moving clockwise while the one to right is moving counterclockwise. The motion of the enemy soldiers over a series of frames is seen by the white linear tracks which show their progress around their respective square trajectories.

Figure 9 shows the latest form of the C130 dashboard. An additional view, the Threat Analysis view, is shown at top right. It is the same as the selected camera view but shows the results of the SIFT feature extraction and the LK optical flow analysis. For local motions that exceed a certain threshold, an indication of "*Threat detected!*" is shown on the mission log.

Figure 9. C-130 Dashboard Incorporating Threat Detection

This work allows for exploration of bidirectional decision making and learning. Initial threat detection may be performed either by a human operating the dashboard or by a cyber agent using camera image processing and feature detection. We expect to look at the following possibilities:

- When a cyber agent detects a threat, the human overseer is alerted and either confirms or denies that an actual threat is present.
- When the human detects a threat, this implies that the threat was not detected by a cyber agent.

In both cases, the cyber threat detection algorithm has the opportunity to learn and increase its accuracy over time. (It should be noted that the ability of humans to detect threats may be enhanced by display of computed artifacts such as color enhancement of moving pixels, possibly labeled by computed velocities, along the lines of a heads-up display.)

The work can potentially further elucidate the appropriate allocation of tasks depending on whether they are better handled by a human or a cyber agent. Cyber agents have advantages such as perfect attention (including analysis of an entire sensor suite at once, whereas a human will at best pay attention to one or two things at a time and at worst be distracted at a key moment); exact computation of sensor-derived quantities such as speed of motion and size of observed phenomenon, whereas a human will estimate these; and high-accuracy control of well-sensed processes. On the other hand, human agents have advantages in pattern recognition, such as classifying a phenomenon as a threat or as no threat, whereas computers may not know

to ignore things like plumes of steam or fog. Moreover, a human is often able to see instantly what kind of physical maneuver is needed, using rapid parallel prediction of multiple possibilities; one need only think of a football quarterback reading the entire field, choosing the receiver, and throwing the ball, all in the space of one or two seconds.

AGENT-IN-THE-LOOP

The agent-in-the-loop learning from a human supervisor involves the integration of a decision tree within the simulation dashboard. The decision tree is invoked whenever a moving object is seen within the field of view of the active camera. It employs a heuristic based on computed indicators which describe the motion, including direction of motion and changes in direction and speed. The result of the decision tree analysis is a choice of three outcomes: the moving object is friendly; the object is an enemy; or the human supervisor should be consulted. See figure 10.

Figure 10. Decision Tree Correctly Identifies Enemy Soldier

In figure 10, a simulated enemy soldier is sent on a time-varying trajectory that leads him towards the parked aircraft. The soldier enters the field of view of the currently active quadcopter, which is observing from a hovered position at altitude 36 meters. The decision tree makes the correct identification of the soldier as an enemy.

A simulated friendly soldier is set to patrol the perimeter of the aircraft. In figure 11, this soldier is correctly identified as friendly, while in figure 12, the decision tree does not reach a conclusion and alerts the human supervisor. In the latter case the supervisor makes the identification, which is recorded as part of the log and used later for learning.

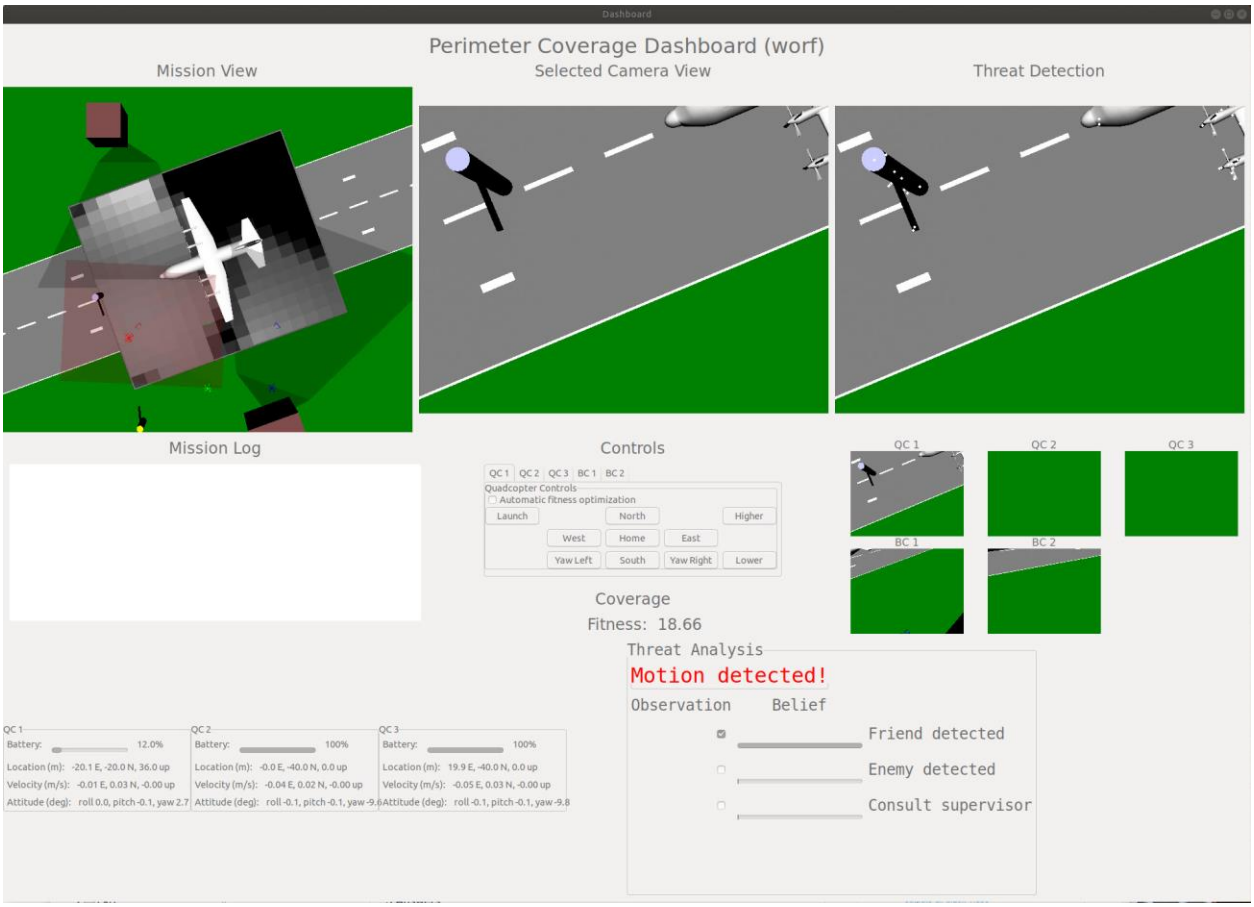

Figure 11. Correct Identification of Friendly Soldier

Figure 12. Identification Requested from the Human Supervisor

This work is intended to present the concept for identification of friend or foe (i.e., it is not meant to be a realistic representation of how this identification is done). In other words, it is a demonstration of the kinds of interaction between an automated agent and a human supervisor, in which the human can correct the agent's work while allowing for learning.

In the work reported on here, learning, i.e. improvement in the classification performance using the decision tree, was achieved offline, by recording details of both correct and incorrect identifications as well as the supervisor classifications. Figure 13 shows the comparison between the performance of the decision tree before and after tuning the structure and parameters of the decision making in the tree. The ROC curve and the confusion matrix in the figure illustrates how misclassification (e.g., identifying an enemy as friend) has been improved. In future work, this approach will be incorporated into online learning in which the decision tree parameters are changed in real time as a result of its performance over time.

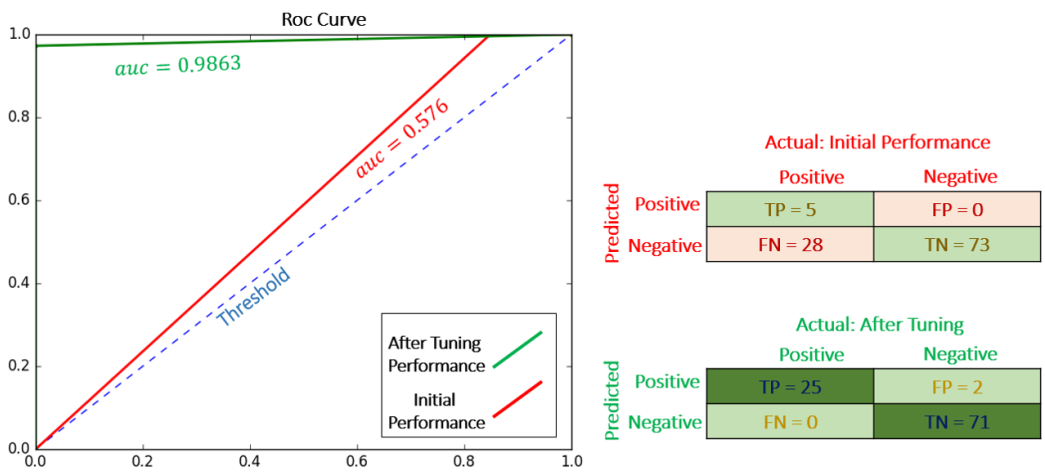

Figure 13. Performance Comparison of Decision Tree after Tuning

CONCLUSION

Adaptive CPHS are CPHS that are capable of adapting to systemic malfunctions or external disruptions using pre-determined rules and machine learning techniques. Examples of adaptive CPHS are smart grids, smart cities, self-driving vehicle networks, smart buildings, as well as any instrumented device that require adaptive response based on context. Three important challenges in adaptive CPHS are learning (with incoming evidence), adaptation to disruptions, and inserting human-in-the-loop at appropriate levels. An illustrative problem of interest to DoD was used to convey key concepts in adaptive CPHS. The problem pertains to maintaining perimeter security of a C-130 aircraft parked on an airstrip at a military outpost. The aircraft is secured by video cameras on buildings in the immediate vicinity and a team of quadcopters with downward facing cameras. In the scenario, the quadcopters are launched from a distant location and have to fly to the surveillance area with partial observability and environment uncertainty. Once at the surveillance area, the quadcopters have full visibility and fly a pattern that maximizes coverage of the aircraft perimeter. The modeling approach employed to cover the phase starting from the launch to the surveillance area in a partially observable environment is POMDP. At the surveillance area, observability is no longer an issue, and the quadcopters are required to fly surveillance patterns that jointly maximize perimeter coverage. When disruption occurs (e.g., one quadcopter has to land because of low battery power), the remaining quadcopters change their altitudes to restore lost coverage. If that adaptive maneuver does not restore coverage, a backup quadcopter is requested. The human supervisor may provide the backup to restore coverage or not. Through this scenario, we have shown how the quadcopters can operate under human supervisory control, or autonomously. We have shown how the underlying model can change from a complex model to a simpler model as a function of problem complexity and environment observability. In this regard, we leveraged our modeling work from RT-166 and RT-210. We have shown the importance of a context-aware dashboard in maximizing human situation awareness, debugging vehicle behaviors, and exploring a variety of what-if situations. The concurrent creation of the models and testbed had several advantages. First, they enabled rapid iterations on the design of the dashboard. Second, the dashboard became an essential aspect of the adaptive CPHS as well as a debugging aid for system behaviors. Third, we were able

to give early demonstrations of the evolving system to DoD, SERC community, and potential customers. At this point, we have gained enough knowledge and experience to create a MBSE testbed for use by members of the SERC research community and beyond. We are in the process of transferring rudimentary testbed and attendant capabilities created during the performance of this RT and RT-210 to The Aerospace Corporation. In transitioning this technology, we acknowledge the Government's intellectual property rights; contract clauses DFARS 252.227-7013 and 252.227-7014.

REFERENCES

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.

Madni, A.M. "The Role of Human Factors in Expert Systems Design and Acceptance," *Human Factors Journal*, August 1988, 30(4), 395-414.

Madni, A.M. "HUMANE: A Designer's Assistant for Modeling and Evaluating Function Allocation Options," *Proceedings of Ergonomics of Advanced Manufacturing and Automated Systems Conference*, Louisville, KY, August 16-18, 1988, pp. 291-302.

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. "Mutual Adaptation in Human-Machine Teams," Intelligent Systems Technology, Inc., Document No.: ISTI-WP-02-012017, January 11, 2017.

Madni, A.M. "Formal Methods for Intelligent Systems Design and Control," AIAA SciTech Forum, 2018 AIAA Information Systems, AIAA InfoTech@Aerospace, Kissimmee, Florida, January 8-12, 2018.

Madni, A.M., and Freedy, A. Intelligent Interfaces for Human Control of Advanced Automation and Smart Systems in *Human Productivity Enhancement, Training and Human Factors in Systems Design*, Vol. 1, (Ed.: J. Zeidner), pp. 318-331, Praeger, 1986.

Madni, A.M. and Madni, C.C. "Context-driven Collaboration During Mobile C^2 Operations," *Proceedings of The Society for Modeling and Simulation International 2004 Western Simulation Multiconference*, January 18-22, 2004, San Diego, CA.

Madni, A.M., and Madni, C.C. Architectural Framework for Exploring Adaptive Human-Machine Teaming Options in Simulated Dynamic Environments, MDPI *Systems,* special issue on *"Model-Based Systems Engineering,"* December 9, 2018.

Madni, A.M., Sage, A. and Madni, C.C. "Infusion of Cognitive Engineering into Systems Engineering Processes and Practices," *Proceedings of the 2005 IEEE International Conference on Systems, Man, and Cybernetics*, October 10-12, 2005, Hawaii.

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., Samet, M., and Purcell, D. Adaptive Models in *Information Management, Applications in Artificial Intelligence* (Ed.: S. Andriole), Petrocelli Books, Inc., Princeton, NJ, 1985, pp. 279-294.

Madni, A.M., Sievers, M. and Madni, C.C. Adaptive Cyber-Physical-Human Systems: Exploiting Cognitive Modeling and Machine Learning in the Control Loop, *INSIGHT*, Vol. 21, Issue 3, pp. 87-93, 2018.

Madni, A.M. and Sievers, M. "Systems Integration: Key Perspectives, Experiences, and Challenges," *Systems Engineering*, Vol. 17, No. 1, p. 37-51, Spring 2014.

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.

Orellana, D. and Madni, A. "Analyzing Human Machine Interaction and Interfaces through Model Based System Engineering Practices," *Proceedings INCOSE International Symposium*, 9-12 July, Rome, Italy, 2012.

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.