CPS: Synergy: Collaborative Research: Engineering Safety-Critical Cyber-Physical-Human Systems

Alex Kirlik, Naira Hovakimyan, Lui Sha, Carolyn Beck, and Xiaofeng Wang

Introduction

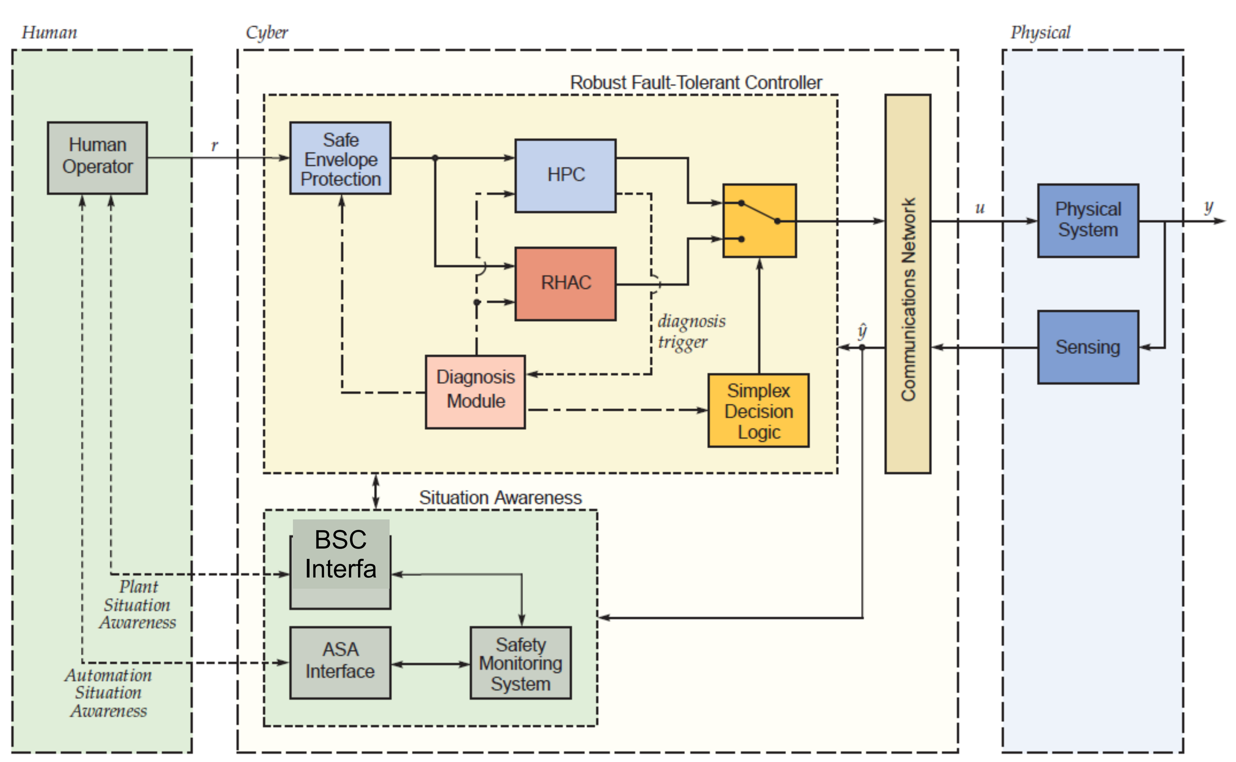
The project addresses fundamental problems in the target areas of engineering of cyber-physical systems with humans in the loop. In Cyber-Physical-Human (CPH) Systems, automation and humans cooperate to achieve high levels of safety and performance.

Objectives:

- The design and evaluation of robust fault-tolerant control (RFTC) systems yielding enhanced levels of safety in highly unpredictable environments.
- The design and implementation of control techniques designed to maintain system operation within safety envelopes or best practices.
- The development and validation of human-automation interaction and interface design techniques to maximize operator situation awareness.

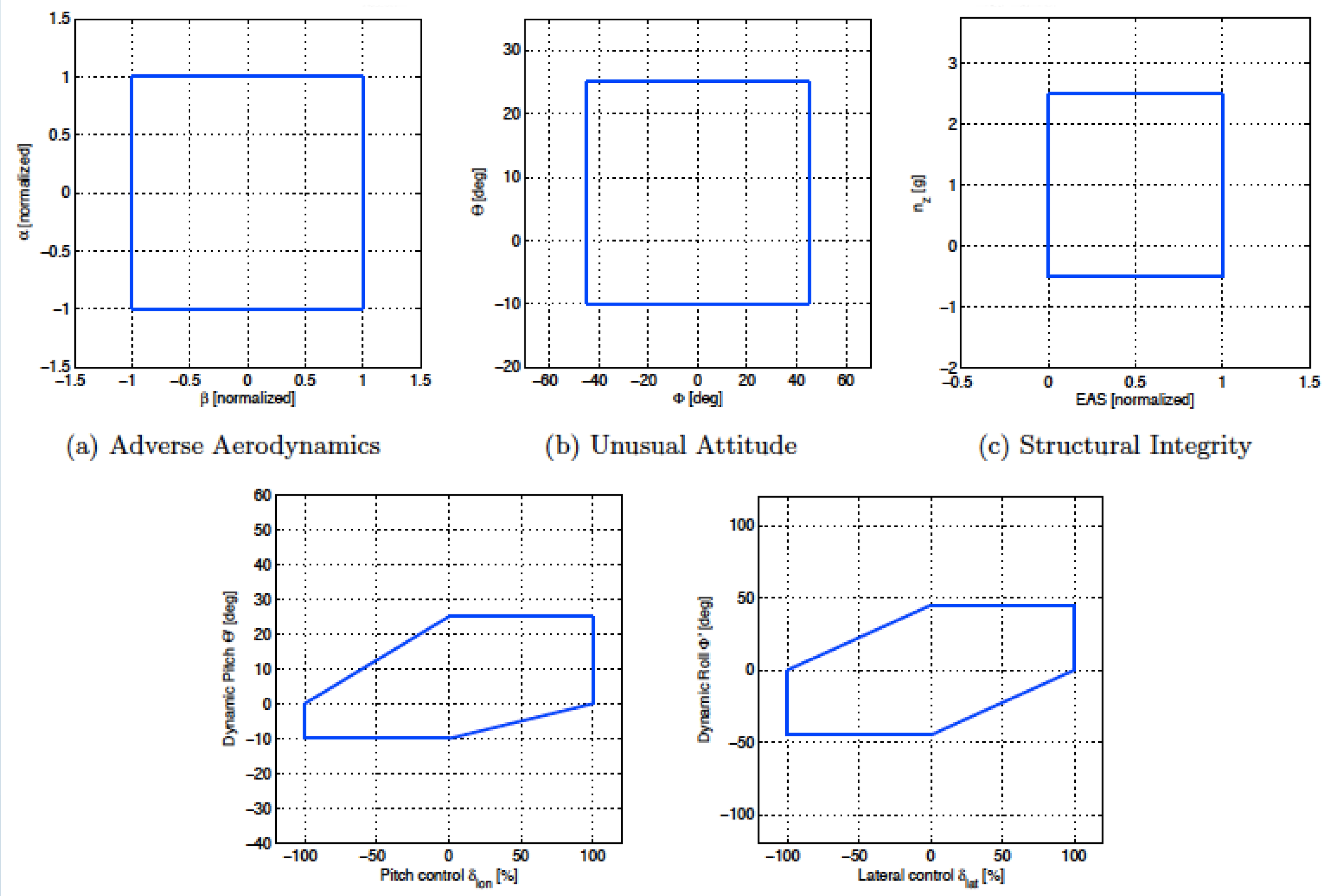
This research will close a key gap by developing formal techniques and best practices for designing and evaluating partially-automated CPH systems to achieve levels of safety and performance beyond what could be achieved by either human expertise or automation acting alone.

Human-Automation-Plant Architecture



- *Safe Envelope Protection*: guarantee the physical system within safe operational limits.
- *High Performance Controller (HPC): d*esigned for a nominal physical system with the purpose of optimizing system performance.
- *Robust High Assurance Controller (RHAC):* provide basic functionalities for safe operation.
- *Decision Logic*: determine when to switch from the HPC to the RHAC.
- *Diagnosis Module*: responsible for fault detection and isolation (FDI) and controller reconfiguration.
- *Safety Monitoring System (SMS) and Situation Awareness (SA) Aids:* ensure **system behavior and automation compensation is transparent** to the operator, including *Automation Situation Awareness (ASA)* and *Behavior Shaping Constraints (BSC)*.

Quantifying Loss-of-Control Safety Envelopes

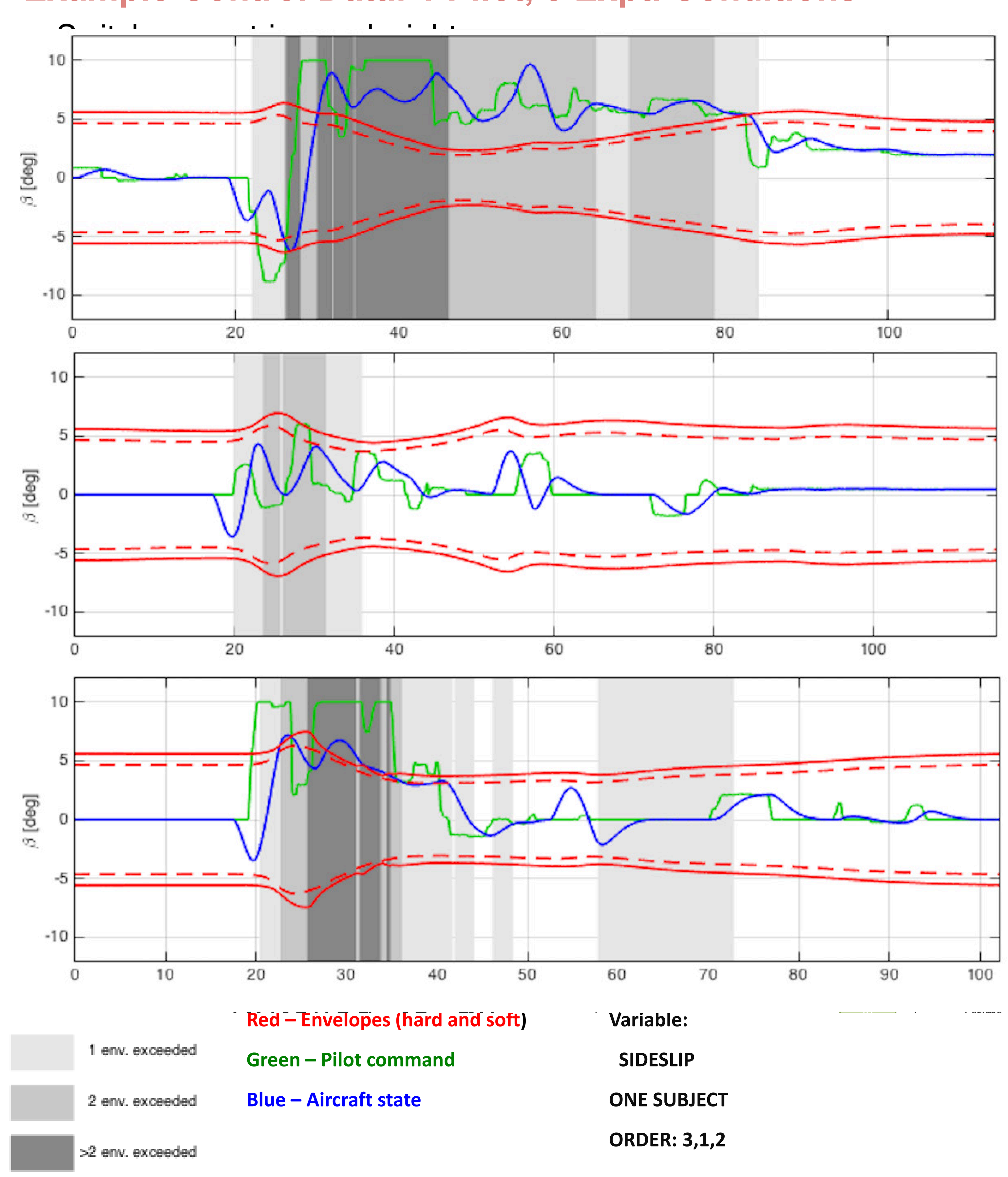


(a) Adverse Aerodynamics (b) Unusual Attitude (c) Structural Integrity

(d) Dynamic Pitch Control (e) Dynamic Roll Control

Loss-of-Control Envelopes (after Wilborn & Foster, 2004)

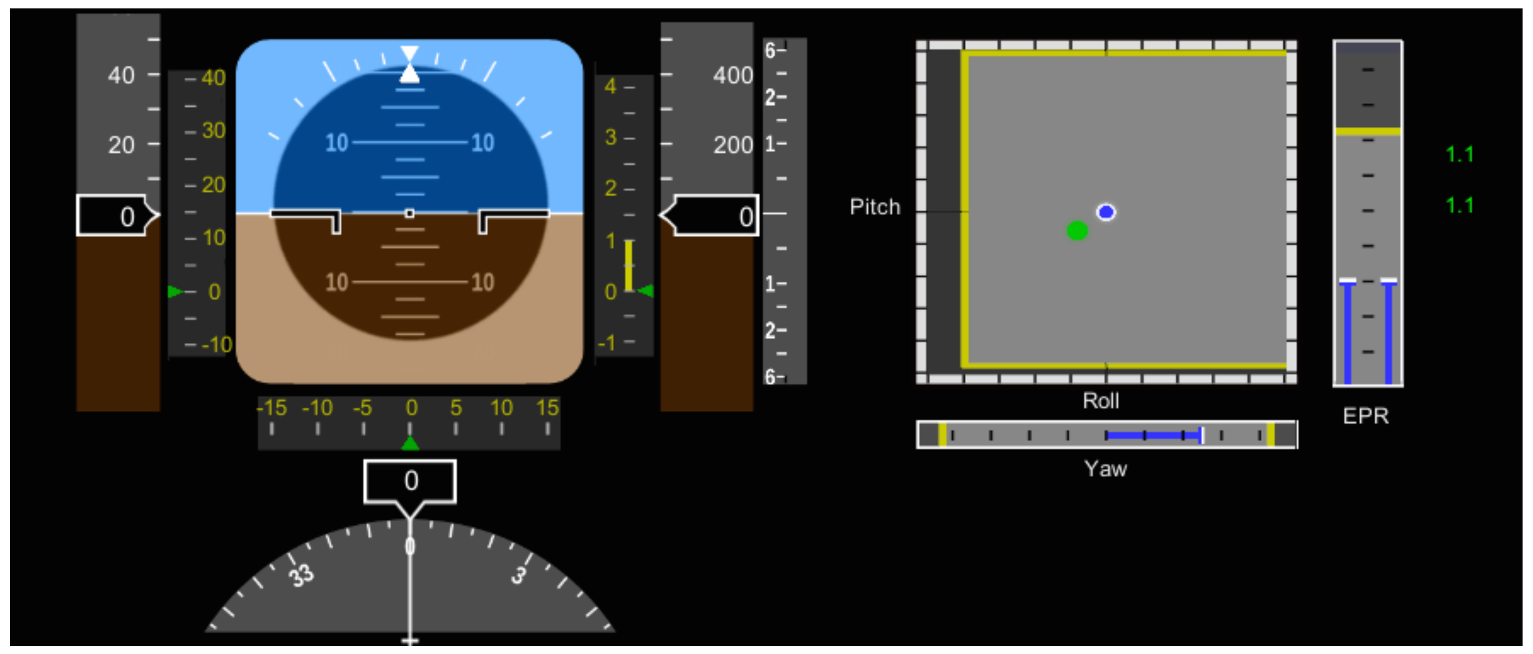
Example Control Data: 1 Pilot, 3 Expt. Conditions



Scenario: Windshear onset 20s into scenario. Conditions: Top - Control. Middle -Display Augmentation. Bottom: Display + Control Augmentation.

The facilities at the Beckman Institute Illinois Simulator are used as an experimental platform to validate the research findings in a realistic pilot-in-the-loop flight scenario.

Interface Design Approach



We are currently developing display methods and simulator scenarios to gauge pilot situational awareness and address the concerns voiced. This will be done through two techniques.

i. Display information about the state of adaptive control automation and the degree it is providing active assistance. (e.g. engaged, magnitude of influence, direction of influence)

ii. Visualization of **behavior shaping constraints** on system state. (e.g. loss of control envelopes, envelope excursion status)

By focusing on maximally informing the pilots with an accurate model of plant and automation state, we allow them to more fully utilize their expert knowledge.

Summary

One unintended side effect of introducing increasingly powerful, often opaque control automation into vehicles such as aircraft and automobiles is that human operators lose situation awareness and cannot be counted on to readily and reliably re-enter the control loop when necessary.

The gist of this project to date has been to re-purpose information provided by control automation used for safety envelope protection from purely closed-loop control augmentation to the design of novel interfaces that allow humans to actively remain in the loop while still benefiting by the guidance provided by this automation.