CALL FOR PAPERS

IEEE Transactions on Emerging Topics in Computational Intelligence

Special Issue on Computational Intelligence for Human-in-the-Loop Cyber Physical Systems

I. Aim and Scope

Recent advances in computational intelligence, real-time computing and control, have given momentum to Human-in-the-Loop Cyber Physical Systems (HitLCPS) to enable game-changing communication and collaboration paradigms that operate in connection with humans' natural behavior patterns. Despite the ongoing advancement of computational intelligence techniques for analyzing the interactions between the cognitive and cyber domains, there are growing concerns regarding the security, privacy, and safety of human when they interact with smart cyber physical environments. The large-scale integration of heterogeneous IoT devices to manage and control a wide variety of sensors and settings will hugely increase the attack surface, the scope for misconfigurations, and hence unsafe or conflicting behavior of various devices and subsystems, which in turn can place the human in unsafe and hazardous situations, both mentally and physically. It is still unclear how to design optimized relationships between people and machines in a scalable manner, how to design triggers for proactive engagement and disengagement, and how to handle the consequences of implied actions. For example, when the system misbehaves as a result of erroneous data, it is important to have real-time rules that can guarantee a fail-safe state for the HitLCPS. The verification of operations in a large HitLCPS can be very complex due to the evolving nature of human-in-the-loop networks both in terms of physical aspects and operational environment. Therefore, understanding the semantics of HitLCPS and the context of control behavior is critical to dispose incorrect configurations and build a proactive resilience and a reactive defense against evolving threats.

To address the above-mentioned challenges, there is a need for new algorithmic developments beyond traditional topics in neural networks, evolutionary computation, and fuzzy systems. The aim of this special issue is to provide a multi-aspect up-to-date reference for theoretical development of computational intelligence techniques for improving "security, privacy, and safety" in emerging HitLCPS applications.

II. Topics

The topics of interest for this special issue include, but are not limited to

- Computational intelligence for security hardening of HitLCPS
- Computational intelligence for integration of communications and sensing in HitLCPS
- Computational models for trusted HitLCPS
- Artificial intelligence safety for HitLCPS
- Explainable human-in-the-loop artificial intelligence
- Explainable decision making for HitLCPS operating in uncertain and evolving environments
- Optimizing safety and security of HitLCPS using evolutionary techniques
- Trusted machine/deep learning for HitLCPS
- Computational intelligence for depicting human vulnerabilities in HitLCPS
- Computational intelligence for resilient HitLCPS
- Innovative computational intelligence techniques for cyber and cyber-physical attacks detection, prevention, and mitigation in HitLCPS applications
- Theoretical development of HitLCPS
- Nature-inspired computational intelligence algorithms for HitLCPS
- Applications of computational intelligence for safe and secure HitLCPS

III. Submissions

Manuscripts should be prepared according to the "Information for Authors" section of the journal, and submissions should be done through the journal submission website: https://mc.manuscriptcentral.com/tetci-ieee, by selecting the Manuscript Type of "Computational Intelligence for Human-in-the-Loop Cyber Physical Systems" and clearly marking "Computational Intelligence for Human-in-the-Loop Cyber Physical Systems" as comments to the Editor-in-Chief. Submitted papers will be reviewed by at least three different reviewers. Submission of a manuscript implies that it is the authors' original unpublished work and is not being submitted for possible publication elsewhere.

IV. Important Dates

Paper submission deadline: **April 15, 2020**
Notice of the first round review results: June 15, 2020
Revision due: August 15, 2020
Final notice of acceptance/reject: October 15, 2020

V. Guest Editors

- Alireza Jolfaei, Macquarie University, Australia
  alireza.jolfaei@mq.edu.au
- Muhammad Usman, University of South Wales, United Kingdom
  muhammad.usman@southwales.ac.uk
- Manuel Roveri, Politecnico di Milano, Milano, Italy
  manuel.roveri@polimi.it
- Michael Sheng, Macquarie University, Australia
  michael.sheng@mq.edu.au
- Marimuthu Palaniswami, University of Melbourne, Australia
  palani@unimelb.edu.au
- Krishna Kant, Temple University, USA
  kkant@temple.edu