

# 2024 ACM/IEEE 15th International Conference on Cyber-Physical Systems (ICCPs) **ICCPs 2024**

## Table of Contents

Message from the ICCPS 2024 Program Chairs .....	x
ICCPs 2024 Organizers .....	xii

### Session 1: Learning-Enabled CPS

Repairing Learning-Enabled Controllers While Preserving What Works .....	1
<i>Pengyuan Lu (University of Pennsylvania, USA), Matthew Cleaveland (University of Pennsylvania, USA), Oleg Sokolsky (University of Pennsylvania, USA), Insup Lee (University of Pennsylvania, USA), and Ivan Ruchkin (University of Florida, USA)</i>	
Zero-One Attack: Degrading Closed-Loop Neural Network Control Systems using State-Time Perturbations .....	12
<i>Stanley Bak (Stony Brook University, USA), Sergiy Bogomolov (Newcastle University, USA), Abdelrahman Hekal (Newcastle University, USA), Veena Krish (Stony Brook University, USA), Andrew Mata (Stony Brook University, USA), and Amir Rahmati (Stony Brook University, USA)</i>	
Attention-Based Real-Time Defenses for Physical Adversarial Attacks in Vision Applications.....	23
<i>Giulio Rossolini (Scuola Superiore Sant'Anna, Italy), Alessandro Biondi (Scuola Superiore Sant'Anna, Italy), and Giorgio Buttazzo (Scuola Superiore Sant'Anna, Italy)</i>	

### Session 2: CPS Security

Thinking Beyond Bus-off: Targeted Control Falsification in CAN .....	33
<i>Ipsita Koley (Indian Institute of Technology Kharagpur, India), Sunandan Adhikary (Indian Institute of Technology Kharagpur, India), and Soumyajit Dey (Indian Institute of Technology Kharagpur, India)</i>	
Rampo: A CEGAR-Based Integration of Binary Code Analysis and System Falsification for Cyber-Kinetic Vulnerability Detection .....	45
<i>Kohei Tsujio (University of California, Irvine), Mohammad Abdullah Al Faruque (University of California, Irvine), and Yasser Shoukry (University of California, Irvine)</i>	

Enhancing Power Grid Resilience to Cyber-Physical Attacks using Distributed Retail Electricity Markets .....	55
<i>Vineet Jagadeesan Nair (Massachusetts Institute of Technology, USA), Priyank Srivastava (Indian Institute of Technology Delhi, India), and Anuradha Annaswamy (Massachusetts Institute of Technology, USA)</i>	

## Session 3: Reinforcement Learning for CPS

Optimal Runtime Assurance via Reinforcement Learning .....	67
<i>Kristina Miller (University of Illinois Urbana-Champaign, USA), Christopher K. Zeitler (Rational CyPhy Inc., USA), William Shen (University of Illinois Urbana-Champaign, USA), Kerianne Hobbs (Air Force Research Laboratory, USA), John Schierman (Air Force Research Laboratory, USA), Mahesh Viswanathan (University of Illinois Urbana-Champaign, USA), and Sayan Mitra (University of Illinois Urbana-Champaign, USA)</i>	
Vulnerability Analysis for Safe Reinforcement Learning in Cyber-Physical Systems .....	77
<i>Shixiong Jiang (University of Notre Dame), Mengyu Liu (University of Notre Dame), and Fanxin Kong (University of Notre Dame)</i>	
FAIRO: Fairness-Aware Sequential Decision Making for Human-in-the-Loop CPS .....	87
<i>Tianyu Zhao (University of California, Irvine), Mojtaba Taherisadr (University of California, Irvine), and Salma Elmalaki (University of California, Irvine)</i>	

## Session 4: Middleware & Software for CPS

Quantitative Safety-Driven Co-Synthesis of Cyber-Physical System Implementations .....	99
<i>Clara Hobbs (The University of North Carolina at Chapel Hill, USA), Shengjie Xu (The University of North Carolina at Chapel Hill, USA), Bineet Ghosh (The University of Alabama, USA), Enrico Fraccaroli (The University of North Carolina at Chapel Hill, USA), Parasara Sridhar Duggirala (The University of North Carolina at Chapel Hill, USA), and Samarjit Chakraborty (The University of North Carolina at Chapel Hill, USA)</i>	
Playground, A Safe Building Operating System .....	111
<i>Xiaohan Fu (University of California San Diego, USA), Yihao Liu (Nanyang Technology University, Singapore), Jason Koh (Mapped, USA), Dezhi Hong (Amazon, USA), Rajesh Gupta (University of California San Diego, USA), and Gabe Fierro (Colorado School of Mines, USA)</i>	
Formally Verified C Code Generation from Hybrid Communicating Sequential Processes .....	123
<i>Shuling Wang (Institute of Software, Chinese Academy of Sciences, China), Zekun Ji (Institute of Software, Chinese Academy of Sciences, China), Xiong Xu (Institute of Software, Chinese Academy of Sciences, China), Bohua Zhan (Institute of Software, Chinese Academy of Sciences, China), Qiang Gao (Institute of Software, Chinese Academy of Sciences, China), and Naijun Zhan (Institute of Software, Chinese Academy of Sciences, China)</i>	

## Session 5: Autonomous Vehicles & Transportation

Sensor Data Transplantation for Redundant Hardware Switchover in Micro Autonomous Vehicles	135
<i>Cailani Lemieux-Mack (Vanderbilt University), Kevin Leach (Vanderbilt University), and Kevin Angstadt (St. Lawrence University)</i>	
A Middle Way to Traffic Enlightenment	147
<i>Matthew Nice (Vanderbilt University, USA), George Gunter (Vanderbilt University, USA), Junyi Ji (Vanderbilt University, USA), Yuhang Zhang (Vanderbilt University, USA), Matthew Bunting (Vanderbilt University, USA), William Barbour (Vanderbilt University, USA), Jonathan Sprinkle (Vanderbilt University, USA), and Daniel Work (Vanderbilt University, USA)</i>	
An Online Approach to Solving Public Transit Stationing and Dispatch Problem	157
<i>Jose Paolo Talusan (Vanderbilt University, USA), Chaeun Han (Pennsylvania State University, USA), Ayan Mukhopadhyay (Vanderbilt University, USA), Aron Laszka (Pennsylvania State University, USA), Dan Freudberg (WeGo Public Transit, USA), and Abhishek Dubey (Vanderbilt University, USA)</i>	

## Session 6: Verification & Control for CPS

Robust Conformal Prediction for STL Runtime Verification Under Distribution Shift	169
<i>Yiqi Zhao (University of Southern California, USA), Bardh Hoxha (Toyota NA R&amp;D, USA), Georgios Fainekos (Toyota NA R&amp;D, USA), Jyotirmoy V. Deshmukh (University of Southern California, USA), and Lars Lindemann (University of Southern California, USA)</i>	
An Online Planning Framework for Multi-Robot Systems with LTL Specification	180
<i>Rohit Singh (Indian Institute of Technology Kanpur, India) and Indranil Saha (Indian Institute of Technology Kanpur, India)</i>	
Control over Low-Power Wide-Area Networks	192
<i>Aakriti Jain (Wayne State University, USA), Prashant Modekurthy (University of Nevada Las Vegas, USA), and Abusayeed Saifullah (Wayne State University, USA)</i>	

## Session 7: Human-Centric and Medical CPS

FinA: Fairness of Adverse Effects in Decision-Making of Human-Cyber-Physical-System	202
<i>Tianyu Zhao (University of California, Irvine) and Salma Elmalaki (University of California, Irvine)</i>	
Curating Naturally Adversarial Datasets for Learning-Enabled Medical Cyber-Physical Systems	212
<i>Sydney Pugh (University of Pennsylvania, Philadelphia), Ivan Ruchkin (University of Florida, Gainesville), James Weimer (Vanderbilt University, Nashville), and Insup Lee (University of Pennsylvania, Philadelphia)</i>	
$\epsilon$ -Neural Thompson Sampling of Deep Brain Stimulation for Parkinson Disease Treatment	224
<i>Hao-Lun Hsu (Duke University, USA), Qitong Gao (Duke University, USA), and Miroslav Pajic (Duke University, USA)</i>	

## Session 8: Industrial Applications

Towards Deterministic End-to-end Latency for Medical AI Systems in NVIDIA Holoscan .....	235
<i>Soham Sinha (NVIDIA, USA), Shekhar Dwivedi (NVIDIA, USA), and Mahdi Azizian (NVIDIA, USA)</i>	
Control Corruption Without Firmware Infection: Stealthy Supply Chain Attacks via PLC Hardware Implants (MalTag) .....	247
<i>Mingbo Zhang (Rutgers University) and Saman Zonouz (Georgia Tech)</i>	
Unsafe Events Detection in Smart Water Meter Infrastructure via Noise-Resilient Learning .....	259
<i>Ayanfeoluwa Oluyomi (Missouri University of Science and Technology, USA), Sahar Abedzadeh (Western Michigan University, USA), Shameek Bhattacharjee (Western Michigan University, USA), and Sajal K. Das (Missouri University of Science and Technology, USA)</i>	

## Poster/Demo Session

Demo Abstract: Playground, A Safe Building Operating System .....	271
<i>Xiaohan Fu (University of California San Diego, USA), Yihao Liu (Nanyang Technological University, Singapore), Jason Koh (Mapped, USA), Dezhi Hong (Amazon, USA), Rajesh Gupta (University of California San Diego, USA), and Gabe Fierro (Colorado School of Mines, USA)</i>	
Iterative Model Checking for Safety-Critical Problems in Cyber-Physical Systems .....	273
<i>Guangyao Chen (ShanghaiTech University, China) and Zhihao Jiang (ShanghaiTech University, China)</i>	
Poster Abstract of Digital-twin-based Decision Support During Personalized Robotic Rehabilitation .....	275
<i>Yilun Chen (ShanghaiTech University, China), Zhuo Jian (ZD Medtech, China), Yixi Wang (ZD Medtech, China), and Zhihao Jiang (ShanghaiTech University, China)</i>	
Multi-Agent System for Optimizing Victim Tagging in Human/Autonomous Responder Teams ....	277
<i>Maria Cardei (University of Virginia, USA) and Afsaneh Doryab (University of Virginia, USA)</i>	
Achieving Real-Time Visual Tracking with Low-Cost Edge AI .....	279
<i>Van Minh Do (Nanyang Technological University, Singapore), Meiqing Wu (Nanyang Technological University, Singapore), Siew-Kei Lam (Nanyang Technological University, Singapore), and Thambipillai Srikanthan (Nanyang Technological University, Singapore)</i>	
Poster Abstract: Landing-Type Aware Multi-Drone Route Generation for Last-Mile Delivery Service .....	281
<i>JiHyun Kwon (DGIST, South Korea), BaekGyu Kim (DGIST, South Korea), Yi-Ying Chen (National Taiwan University, Taiwan), and Chung-Wei Lin (National Taiwan University, Taiwan)</i>	

Poster Abstract: Signal Temporal Logic Compliant Motion Planning using Reinforcement Learning .....	283
<i>Tushar Dilip Kurne (Indian Institute of Science, India), Manas Sashank Juvvi (Indian Institute of Science, India), Vaishnavi J (Indian Institute of Science, India), and Pushpak Jagtap (Indian Institute of Science, India)</i>	
Adaptive Protection of Power Grids Against Stealthy Load Alterations .....	285
<i>Anjana Balabhaskara (Indian Institute of Technology Kharagpur, India), Sunandan Adhikary (Indian Institute of Technology Kharagpur, India), Ipsita Koley (Indian Institute of Technology Kharagpur, India), Soumyajit Dey (Indian Institute of Technology Kharagpur, India), and Ashish R. Hota (Indian Institute of Technology Kharagpur, India)</i>	
Poster Abstract: Assuring LLM-Enabled Cyber-Physical Systems .....	287
<i>Weizhe Xu (University of Notre Dame, USA), Mengyu Liu (University of Notre Dame, USA), Steven Drager (Air Force Research Laboratory, USA), Matthew Anderson (Air Force Research Laboratory, USA), and Fanxin Kong (University of Notre Dame, USA)</i>	
Poster Abstract: Neural Architecture Sizing for Autonomous Systems .....	289
<i>Shengjie Xu (The University of North Carolina at Chapel Hill, USA), Clara Hobbs (The University of North Carolina at Chapel Hill, USA), Yukai Song (University of Pittsburgh, USA), Bineet Ghosh (The University of Alabama, USA), Sharmin Aktar (The University of North Carolina at Chapel Hill, USA), Lei Yang (George Mason University, USA), Yi Sheng (George Mason University, USA), Weiwen Jiang (George Mason University, USA), Jingtong Hu (University of Pittsburgh, USA), Parasara Sridhar Duggirala (The University of North Carolina at Chapel Hill, USA), and Samarjit Chakraborty (The University of North Carolina at Chapel Hill, USA)</i>	
Author Index .....	291